CMS Manual System	Department of Health & Human Services (DHHS)
Pub 100-17 Medicare Business Partners Systems Security	Centers for Medicare & Medicaid Services (CMS)
Transmittal 9	Date: June 20, 2008
	Change Request 5976

Subject: CMS Business Partner Systems Security Manual

I. SUMMARY OF CHANGES: The BPSSM was updated to reflect changes in NIST, OMB and HHS requirements.

New / Revised Material Effective Date: July 1, 2008 Implementation Date: July 22, 2008

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated) R=REVISED, N=NEW, D=DELETED-*Only One Per Row.*

R/N/D	Chapter / Section / Subsection / Title
R	Record of Changes
R	Table of Contents
R	1/Introduction
R	1.1/Additional Requirements for MAC Contractors
R	2/IT Systems Security Roles and Responsibilities
R	2.1/CMS Project Officer (PO)
R	2.2/The (Principal)Systems Security Officer (SSO)
R	2.3/Business Owners
R	2.4/System Maintainers/Developers
R	2.5/Personnel Security/Suitability
R	3/IT Systems Security Program Management
R	3.1/System Security Plan (SSP)
R	3.2/Risk Assessment
R	3.3/Certification
R	3.4/Information Technology (IT) Systems Contingency Plan

R	3.5.2/Annual FISMA Evaluation (FE)
D	3.5.2.1/Background
D	3.5.2.2/POAandM Package Components/Submission Format
R	3.5.3/Plan of Action and Milestones (POAandMs)
N	3.5.3.1/Background
N	3.5.3.2/POAandM Package Components/Submission Format
N	3.5.4/Annual/Yearly Compliance Condition
R	3.6/Incident Reporting and Response
R	3.6.1/Computer Security Incident Response
R	3.7/System Security Profile
R	3.10.1/Security Configuration Management
R	3.10.2/National Institute of Standards and Technology (NIST)
R	4.1/Security Objectives
R	4.1.1/Potential Security Impact Levels
R	4.1.2/Security Levels by Information Type
R	4.1.3/CMS Security Level Designation-HIGH
N	4.1.4/Minimum System Security Requirements-HIGH
R	4.2/Sensitive Information Protection Requirements
R	4.2.1/Restricted Area
R	4.2.2/Security Room
R	4.2.3/Secured Areas (Secured Interior / Secured Perimeter)
R	4.2/4.2.4/Containers
R	4.2.4.1/Locked Container
R	4.2.4.2/Security Container
R	4.2.4.3/Safes/Vaults
R	4.2.5/Locking Systems
R	4.2.6/Intrusion Detection Systems (IDS)
R	5/Internet Security
R	Appendix A/The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs)
D	Appendix A/Attachment A/ CMS CSRs
N	Appendix A/Attachment 1/CMS Core Security Requirements (CSR) for High Impact Level Assessments

N	Appendix A/Attachment 2/CMS Core Security Requirements (CSR) for Moderate Impact Level Assessments
N	Appendix A/Attachment 3/CMS Core Security Requirements (CSR) for Low Impact Level Assessments
R	Appendix B/Medicare Information Technology (IT) Systems Contingency Planning
R	Appendix D/CMS Information Security (IS) Guidebook for Audits
R	Appendix E/CMS Guidelines
R	Appendix F/Security Configuration Management
R	Appendix G/Acronyms and Abbreviations
R	Appendix H/Glossary

III. FUNDING:

SECTION A: For Fiscal Intermediaries and Carriers:

No additional funding will be provided by CMS; Contractor activities are to be carried out within their operating budgets.

SECTION B: For Medicare Administrative Contractors (MACs):

The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

IV. ATTACHMENTS:

Business Requirements

Manual Instruction

*Unless otherwise specified, the effective date is the date of service.

Attachment – Business Requirements

Pub. 100-17Transmittal: 9Date: June 20, 2008Change Request: CR 5976

SUBJECT: Business Partners Systems Security Manual

Effective Date: July 1, 2008

Implementation Date: July 22, 2008

I. GENERAL INFORMATION

A. Background: The purpose of this updates is to communicate to Medicare Contractors changes to CMS requirements and to incorporate the revision of NIST SP 800-53 as well as OMB mandates. Additionally, the CSRs were updated to reflect the latest changes to NIST SP 800-53 and NIST SP 800-53A.

B. Policy: The policy (s) mandating this change request are the Federal Information Security Management Act of 2002, National Institute of Standards and Technology guidance, and CMS policies, standards, guidelines and procedures.

II. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement

Number	Requirement	Responsibility (place an "X" in each applicable column)									
		A	D	F	C	R		Sha			Other
		/	M	I	A	H		Syst			
		B	Ε		R	H		laint			
		М	М		R	1	F	M	V	C	
		A	A		E		I S	C S	M S	W F	
		C	C		R		s S	3	3	Г	
5976.1	Medicare Contractors shall follow the processes outlined in the Medicare Business Partners Systems Security Manual.	X	X	X		Х	X	X	X	X	X (HIGL AS, EDCs & PSCs)
5976.2	Medicare Contractors shall follow the instructions and guidance when evaluating all CSRs and preparing CSR responses.	X	Х	X	Х	Х	Х	Х	X	X	X (HIGL AS, EDCs & PSCs)

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility (place an "X" in each applicable column)									
		Α	D	F	C	R		Shar			Other
		/	Μ	Ι	A	H		Syst			
		В	Е		R	Η	M	Iainta	ainer	s	
					R	Ι	F	Μ	V	С	
		Μ	Μ		Ι		Ι	С	Μ	W	
		Α	А		E		S	S	S	F	
		С	С		R		S				
	None.										

IV. SUPPORTING INFORMATION

Section A: For any recommendations and supporting information associated with listed requirements, use the box below: N/A

"Should" denotes a recommendation.

X-Ref	Recommendations or other supporting information:
Requireme	
nt	
Number	

Section B: For all other recommendations and supporting information, use this space: N/A

V. CONTACTS

Pre-Implementation Contact(s): Kevin Potter 410.786.5686 and Sherwin Schulterbrandt 410.786.0743

Post-Implementation Contact(s): Kevin Potter 410.786.5686 and Sherwin Schulterbrandt 410.786.0743

VI. FUNDING

Section A: For Fiscal Intermediaries (FIs), Carriers, and Regional Home Health Carriers (RHHIs):

No additional funding will be provided by CMS; contractor activities are to be carried out within their operating budgets.

Section B: For Medicare Administrative Contractors (MACs):

The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

Centers for Medicare & Medicaid Services (CMS)

Business Partners

Systems Security Manual



CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

(Rev. 9, 06-20-08)

CMS/Business Partners Systems Security Manual

Record of Changes

Revision 9	Major Changes Main document and all appendices: Updated to reflect new FISMA Evaluation process and new CMS CSRs.	Date 06/08					
	1 - 1.1: Updated list of document references, titles, and links.						
	2.1: Deleted all references to CCMO.						
	2.2: Deleted reference to Line One funding.						
	2.3: Changed System Owners/Managers to Business Owners.						
	3: Changed Self-Assessment to FISMA Evaluation. Updated Table 3.1 from Self-Assessment to FISMA Evaluation and added and used acronyms where applicable; and added acronyms to Legend and contract type address list. Updated footnote titles. Deleted Consortia contact and address information and all CCMO references.						
	3.1: Changed System Owners/Managers to Business Owners. Updated document titles and links.						
	3.2: Updated document titles and links.						
	3.3: Changed Self-Assessment to FISMA Evaluation.						
	3.3: Clarified backup facility testing when multiple contract types are involved.						
	3.4: Clarified annual testing requirement when multiple Medicare contracts are involved.						
	3.5.2: Added Section 3.5.2, Annual FISMA Evaluation (FE) to explain new FISMA validation requirement.						
	3.5.3 – 3.5.4: Updated section numbers and changed Self-Assessment to FISMA Evaluation.						

3.6: Updated Security Incident definition.

Revision Major Changes

3.6.1: Updated Security Incident response requirements. Added new Table 3.2, Incident Categories, and Table 3.3, Incident Reporting Timeframe Criteria. Updated reference to new CMS incident reporting procedures.

3.7: Changed CISS Self-Assessment to FISMA Evaluation.

3.10.2: Updated Table 3.4, NIST Publications.

4 – 4.1.4: Rewrote section 4.1 and all of its subsections to incorporate FIPS Pub 199 security categorization standards, potential security impact levels, security levels by information type, CMS security level designation—HIGH, and minimum system security requirements—HIGH. Added Table 4.1, System Security Level Definitions, and Table 4.2, FIPS 199 Security Levels by Information Type.

4.2 – 4.2.6: Revised sections to incorporate and clarify revised information protection requirements.

5: Added one exception to the CMS Internet policy allowing the submission of Form 1099 using the IRS FIRE system.

Appendix A: Rewrote most of this appendix to replace the former annual Self-Assessment with the new annual FISMA Evaluation requirement, the new CSR format, and their new response status reporting requirements. Completely rewrote the former CSRs and added separate CSR attachments for: (1) High Impact Level, (2) Moderate Impact Level, and (3) Low Impact Level Assessments.

Appendix B: Added information about the tabletop test and the CMS tabletop test procedures reference.

Appendix D: Clarified CFO/EDP audit information, changed Self-Assessment to FISMA Evaluation, and clarified some acronyms.

Appendix E: Clarified some acronyms, changed Self-Assessment to FISMA Evaluation, and updated some NIST references. Added new whitepapers to appendix.

Appendix F: Clarified some acronyms, and updated some references and their links. Added new section 4.0, HHS

Revision Major Changes

Date

Federal Desktop Core Configuration (FDCC) Standard for Windows XP.

Appendix G: Added new acronyms.

Appendix H: Added new terms and definitions, and updated some existing definitions.

CMS/Business Partners Systems Security Manual

Table of Contents

(Rev. 9, 06-20-08)

- 1 Introduction
- 1.1 Additional Requirements for MAC Contractors 2
 - IT Systems Security Roles and Responsibilities
 - CMS Project Officer (PO) 2.1
 - 2.2 The (Principal) Systems Security Officer (SSO)
 - 2.3 **Business** Owners
 - 2.4 System Maintainers/Developers
 - Personnel Security/Suitability 2.5
- 3 IT Systems Security Program Management
 - System Security Plan (SSP) 3.1
 - 3.2 **Risk Assessment**
 - 3.3 Certification
 - 3.4 Information Technology (IT) Systems Contingency Plan
 - 3.5 Compliance
 - 3.5.1 Annual Compliance Audit (ACA)
 - 3.5.2 Annual FISMA Evaluation (FE)
 - 3.5.3 Plan of Action and Milestones (POA&Ms)
 - 3.5.3.1 Background
 - 3.5.3.2 POA&M Package Components/Submission Format
 - 3.5.4 Annual/Yearly Compliance Condition
 - **Incident Reporting and Response** 3.6
 - 3.6.1 Computer Security Incident Response
 - 3.7 System Security Profile
 - Fraud Control 3.8

4

- 3.9 Patch Management
- 3.10 Security Management Resources
 - 3.10.1 Security Configuration Management
 - 3.10.2 National Institute of Standards and Technology (NIST)
- Information and Information Systems Security Categorization
 - 4.1 Security Impact Levels
 - 4.1.1 Security Objective Potential Impact Levels
 - 4.1.2 CMS Information and Information Systems Security Levels
 - 4.1.3 Criticality Impact Levels for IT Systems
 - 4.2 CMS Sensitive Information Protection Requirements
 - 4.2.1 Restricted Area
 - 4.2.2 Security Room
 - 4.2.3 Secured Interior/Secured Perimeter
 - 4.2.4 Container

- 4.2.4.1 Locked Container
- 4.2.4.2 Security Container
- 4.2.4.3 Safes/Vaults
- 4.2.5 Locking Systems
- 4.2.6 Intrusion Detection Systems (IDS)
- 5 Internet Security

Appendices

- (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)
- Appendix A The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs)

Attachment 1 CMS Core Security Requirements (CSR) for High Impact Level Assessments Attachment 2 CMS Core Security Requirements (CSR) for Moderate Impact Level Assessments Attachment 3 CMS Core Security Requirements (CSR) for Low Impact Level Assessments

Appendix B	Medicare Information Technology (IT) Systems Contingency Planning
Appendix C	An Approach to Fraud Control
Appendix D	CMS Information Security (IS) Guidebook for Audits
Appendix E	CMS Guidelines
Appendix F	Security Configuration Management

- Appendix G Acronyms and Abbreviations
- Appendix H Glossary

1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Centers for Medicare & Medicaid Services (CMS) requires that its business partners implement information technology (IT) systems security controls in order to maintain the confidentiality, integrity, and availability of Medicare systems operations in the event of computer incidents or physical disasters.

A CMS business partner (contractor) is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Medicare carriers, Fiscal Intermediaries, Common Working File (CWF) host sites, standard system maintainers, regional laboratory carriers, claims processing data centers, Data Centers, Enterprise Data Centers (EDCs), and Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC]).

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 -SEC. 912: Requirements for Information Security for Medicare Administrative Contractors" (Section 912 of the MMA) provided for a new type of contractor relationship, the "Medicare Administrative Contractor," and implemented requirements for annual evaluation, testing, and reporting on security programs at both MAC contractors and existing carrier and intermediary business partners (to include their respective data centers). In this manual the terms "business partner" and "contractor" are used interchangeably, and all provisions that apply to business partners also apply to MAC contractors.

This manual addresses the following key business partner security elements:

- An overview of primary roles and responsibilities
- A program management planning table that will assist System Security Officers (SSOs) and other security staff in coordinating system security programs at business partner sites
- Appendix A: The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs), which provides the following:
 - The CSRs
 - o An overview of the CISS data collection and reporting process

The CMS IT systems security program and CSRs were developed in accordance with Federal and CMS documents that mandate the handling and processing of Medicare data. These documents include the following:

• CMS *Information Security (IS)* System Security Plans (SSP) *Procedures*, Version 4.0 *Draft, July 10, 2007*

http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage

- Federal Information Security Management Act of 2002 (FISMA), November 27, 2002
 <u>http://csrc.nist.gov/drivers/documents/FISMA-final.pdf</u>
- Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, Electronic Freedom of Information Act of 1996 <u>http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm</u>
- GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999 <u>http://www.gao.gov/special.pubs/ai12.19.6.pdf</u>
- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies *and Entities*, *February 2007* <u>http://www.irs.gov/pub/irs-pdf/p1075.pdf</u>
- Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (PUBLIC LAW 108–173), DEC. 8, 2003—SEC. 912: Requirements for Information Security for Medicare Administrative Contractors <u>http://frwebgate.access.gpo.gov/cgi-</u> bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ173.108.pdf
- Office of Management and Budget (OMB) Circular No. A-127, Financial Management Systems, June 21, 1995 <u>http://www.whitehouse.gov/omb/circulars/a127/a127.html</u>
- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999
 http://www.whitehouse.gov/omb/circulars/index.html
- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000 <u>http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html</u>
- Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000 <u>http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html</u>
- Presidential Decision Directive/NSC 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998 <u>http://www.usdoj.gov/criminal/cybercrime/white_pr.htm</u>
- Public Law 74-271, Social Security Act, as amended, §1816, Use of public agencies or private organizations to facilitate payment to provider of service

http://www.ssa.gov/OP_Home/ssact/title18/1816.htm

- Public Law 74-271, Social Security Act, as amended, §1842, Use of carriers for administration of benefits <u>http://www.ssa.gov/OP_Home/ssact/title18/1842.htm</u>
- Public Law 93-579, The Privacy Act of 1974, as amended http://www.usdoj.gov/foia/privstat.htm
- Public Law 99-474, Computer Fraud & Abuse Act of 1986 http://nsi.org/Library/Compsec/cfa.txt
- Public Law 100-235, Computer Security Act of 1987 <u>http://www.nist.gov/cfo/legislation/Public Law 100-235.pdf</u>
- Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35 <u>http://www.estrategy.gov/documents/16.pdf</u>
- Public Law 104-106, Clinger-Cohen Act of 1996 (formerly called the Information Technology Management Reform Act) <u>http://www.tricare.osd.mil/jmis/download/PublicLaw104_106ClingerCohenActof</u> <u>1996.pdf</u>
- Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA), 1996
 <u>http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAAlawdetail.pdf</u>

Additional documents were used as references in the development of this manual and the CMS CSRs. These documents include the following:

- CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Version 3.0, September 19, 2007 <u>http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage</u>
- CMS Information Security (IS) Certification and Accreditation (C&A) Program Procedures, Version 3.0.13 Final Draft, June 26, 2007 <u>http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage</u>
- CMS Information Security Risk Assessment (IS RA) Procedures, Version 4.0 Draft, July 23, 2007 <u>http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage</u>
- CMS Information Security Risk Assessment (RA) and System Security Plan (SSP) Guidance, Version 1.0 September 3, 2004

http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPa ge

- Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 Suitability, 5CFR731 http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html
- United States Code Title 44 Chapter 33—Disposal of Records http://www4.law.cornell.edu/uscode/html/uscode44/usc_sup_01_44_10_33.html
- Department of Health and Human Services (HHS), IRM *OCIO* Policies <u>http://www.hhs.gov/read/irmpolicy/index.html</u>
- Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003* http://www.fas.org/irp/offdocs/nspd/hspd-7.html
- Homeland Security Presidential Directive/HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004 <u>http://www.fas.org/irp/offdocs/nspd/hspd-12.html</u>
- Homeland Security Presidential Directive/HSPD-20, National Continuity Policy, May 9, 2007 <u>http://www.fas.org/irp/offdocs/nspd/nspd-51.htm</u>
- Federal Information Processing Standards (FIPS) Publication (PUB) 140-3 Draft, Security Requirements for Cryptographic Modules, July 2007 <u>http://csrc.nist.gov/publications/PubsFIPS.html</u>
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004 <u>http://csrc.nist.gov/publications/PubsFIPS.html</u>
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006 <u>http://csrc.nist.gov/publications/PubsFIPS.html</u>
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995 <u>http://csrc.nist.gov/publications/PubsSPs.html</u>
- NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems, December 2007 <u>http://csrc.nist.gov/publications/PubsSPs.html</u>

- NIST SP 800-53A Final Public Draft, Guide for Assessing the Security Controls in Federal Information Systems, December 2007 <u>http://csrc.nist.gov/publications/PubsSPs.html</u>
- NIST SP 800-61, Computer Security Incident Handling Guide, September 28, 2007
 <u>http://csrc.nist.gov/publications/PubsSPs.html</u>
- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004 <u>http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html</u>.
- CMS Policy for the Information Security Program, CMS-CIO-POL-SEC02-02 Draft, August 24, 2007 <u>http://www.cms.hhs.gov/InformationSecurity/13_Policies.asp#TopOfPage</u>

1.1 Additional Requirements for MAC Contractors

the contract.

(*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

MAC contractors are responsible for fulfilling all existing business partner requirements. Additional requirements are specified in Section 912 of the Medicare Modernization Act (MMA). These additional requirements include the following:

• The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 days of receipt of the final audit or evaluation report, unless otherwise authorized by CMS.

The contractor shall comply with the CMS Certification and Accreditation (C&A) methodology, policies, standards, procedures, and guidelines for contractor facilities and systems. The CMS *IS* C&A *Program Procedures* can be found on the CMS *Web* site at: *http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage*

- The contractor shall conduct or undergo an independent evaluation and test of its system security program in accordance with Section 912 of the MMA. The first test shall be completed before the contractor commences claims payment under
- The contractor shall support CMS validation and accreditation of contractor systems and facilities in accordance with the CMS *IS* C&A *Program Procedures*.

- The contractor shall provide annual certification, in accordance with the CMS *IS* C&A *Program Procedures*, that they have examined the management, operational, and technical controls for its systems supporting the MAC function, and consider these controls adequate to meet CMS security standards and requirements.
- The contractor shall appoint a Chief Information Officer (CIO) to oversee its compliance with the CMS security requirements. The contractor's Systems Security Officer (SSO) shall be a full-time position dedicated to assisting the CIO in fulfilling these requirements.

2 IT Systems Security Roles and Responsibilities

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

2.1 CMS Project Officer (PO)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS POs (generally located in Central Office business components) oversee the other business partners and also have Federal Acquisition Regulation (FAR) responsibilities at data centers. The PO has the following responsibilities:

- CMS point of contact for business partner IT systems security problems
- Central point for the reception of IT SSPs and reports including security incident reports
- Provider of technical assistance necessary to respond to CMS security policies and procedures

2.2 The (Principal) Systems Security Officer (SSO)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners *shall* designate an SSO qualified to manage the Medicare system security program and ensure the implementation of necessary safeguards. The SSO *shall* be organizationally independent of IT operations. The SSO can be within the CIO organizational domain but cannot have responsibility for operation, maintenance, or development.

The SSO position for each contractor should be full-time and fully qualified—preferably credentialed in systems security (e.g., Certified Information Systems Security Professional [CISSP]). Having an individual with appropriate education and experience to execute security administration duties will help reinforce that security must be a cultural norm that guides daily activities, and not a set of compliance directives. A

qualified SSO who is available to direct security operations full-time provides the foundation for the security culture and awareness of the organization.

A sound entity-wide security program is the cornerstone of effective security control implementation and maintenance. Security controls cannot be effective without a robust entity-wide security program that is fully sponsored and practiced by management, and staffed by individuals with proper training and knowledge. Contractors should also encourage their systems security personnel to pursue security accreditation using available funding.

A business partner may have additional SSOs at various organizational levels, but all security actions *shall* be coordinated through the principal SSO for Medicare records and operations. The SSO ensures compliance with CMS CSRs by:

- Facilitating the Medicare IT system security program and ensuring that necessary safeguards are in place and working
- Coordinating system security activities throughout the organization
- Ensuring that IT system security requirements are considered during budget development and execution
- Reviewing compliance of all components with the CMS CSRs and reporting vulnerabilities to management
- Establishing an incident response capability, investigating system security breaches, and reporting significant problems (see section 3.6) to business partner management.
- Ensuring that technical and operational security controls are incorporated into new IT systems by participating in all business planning groups and reviewing all new systems/installations and major changes
- Ensuring that IT systems security requirements are included in Requests for Proposal (RFP) and subcontracts involving the handling, processing, and analysis of Medicare data
- Maintaining systems security documentation in the System Security Profile for review by CMS and external auditors
- Cooperating in all official external evaluations of the business partner's system security program
- Facilitating the completion of the Risk Assessment (see section 3.2)

- Ensuring that an operational IT Systems Contingency Plan is in place and tested (see section 3.4)
- Documenting and updating the monthly Plan of Action and Milestones (POA&M) (see section 3.5.2). Updates may occur whenever a POA&M projected completion date passes, and following the issuance of new requirements, risk assessments, internal audits, and external evaluations. The schedule and updates are highly sensitive and should have limited distribution.
- Keeping all elements of the business partner's System Security Profile secure (see section 3.7)
- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix B)

The Principal SSO should earn a minimum of 40 hours in continuing professional education credits each year from a recognized national information systems security organization. The educational sessions at the CMS Security Best Practices Conference can be used toward fulfilling CMS business partners' continuing professional education credits. The qualifying sessions and associated credit hours will be noted on the CMS Security Best Practices Conference agenda.

2.3 *Business* Owners

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partner **Business** Owners are responsible for:

- Determining and documenting the information and information system security levels of the resources for which they are responsible
- Identifying appropriate security level categorizations for their information and information systems

2.4 System Maintainers/Developers

(*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)* Business partner System Maintainers/Developers have the responsibility to implement the security requirements throughout the System Development Life Cycle (SDLC).

2.5 Personnel Security/Suitability

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All business partner and contractor employees requiring access to CMS sensitive information *shall* meet minimum personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title, and favorable results from a background check. The background check for

prospective and existing employees (if not previously completed) should include, at a minimum: contacting references provided by the employee and contacting the local law enforcement agency or agencies.

3 IT Systems Security Program Management

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners *shall* have policies and procedures, and implement controls or plans that fulfill the CMS CSRs (see *applicable* Attachment).

Policies are formal, up-to-date, documented rules stated as "shall" or "will" statements that exist and are readily available to employees. They establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness. Policies are written to cover all major facilities and operations corporate-wide or for a specific asset (e.g., Medicare claims processing), and they are approved by key affected parties. Policies delineate the IT security management structure, clearly assign IT security responsibilities, and lay the foundation necessary to reliably measure progress and compliance. Policies also identify specific penalties and disciplinary actions to be used in the event that the policy is not followed.

Procedures are formal, up-to-date, documented instructions that are provided to implement the security controls identified by the defined policies. They clarify where the action is to be performed, how the action is to be performed, when the action is to be performed, who is to perform the action, and on what the action is to be performed. Procedures clearly define IT security responsibilities and expected behaviors for: asset owners and users, information resources management and data processing personnel, management, and IT security administrators. Procedures also indicate appropriate individuals to be contacted for further information, guidance, and compliance. Finally, procedures document the implementation of, and the rigor with which, the control is applied.

Controls are measures implemented to protect the confidentiality, integrity, and availability of sensitive information. IT security procedures and controls shall be implemented in a consistent manner everywhere that the procedure applies. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. In addition, initial testing shall be performed to ensure that controls are operating as intended.

Meeting requirements does not validate the quality of a program. Managers with oversight responsibility *shall* understand the processes and methodology behind the requirements. Table 3.1 identifies key requirements and provides high-level descriptions for them. As appropriate, Table 3.1 refers to other parts of this document that provide details on ways to accomplish each requirement. Business partners *shall* perform a *FISMA Evaluation*¹ using the CISS. The weaknesses, action plans, and POA&Ms *shall*

be recorded in the CISS (See Appendix A). To perform the *FISMA Evaluation*, business partners *shall* conduct a systematic review of the CSRs using the CISS. The CISS provides a *FISMA Evaluation* form that includes guidance and audit protocols to assist in the review of the requirements.

The CMS CSRs include key security-related tasks. Table 3.1 indicates how often these tasks need to be performed, the disposition of output or documentation, comments, and a space to indicate completion or a "do by" date. The number accompanying each entry in the requirement column indicates the section in this document that deals with the particular requirement. Use this table as a checklist to ensure that all required IT systems security tasks are completed on schedule. Consult the referenced sections for clarifying details.

Requirement	Frequency	Send To	Comments	Complete (check when complete)
Appendix A, <i>FISMA Evaluation</i> using the CISS	One third of the controls shall be tested each Federal FY so all controls are tested during a three (3) year period.	PO with a copy to CMS COSystem Security Profile	See Appendix A for an overview of the <i>FISMA Evaluation</i> . <i>FISMA Evaluation</i> results recorded using the CISS are to be discussed in the Certification Package.	
3.1 Information Security (IS) System Security Plans (SSP)	The <i>IS</i> SSP for each GSS & MA <i>shall</i> be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change ² .	SSOCMS COSystem Security Profile	<i>IS</i> SSPs are to be reviewed, updated, and certified by management and indicated as such in both the Certification Package/ Statement of Certification and the System Security Profile ³ .	
3.2 Information Security Risk Assessment (IS RA) (Report)	The <i>IS RA</i> for each GSS and MA <i>shall</i> be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change. ¹	 CMS CO System Security Profile 	<i>IS</i> RAs are to be reviewed, updated, and certified by management and indicated as such in both the Certification Package/ Statement of Certification and the System Security Profile. The <i>IS</i> RA Report <i>is</i> submitted with the <i>IS</i> SSP ⁴ .	
3.3 Certification	Each Federal FY	 PO with a copy to CMS CO System Security Profile 	Fiscal intermediaries and carriers should include a statement of certification as part of their CPIC package. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-6) information on certification requirements including where, when, and to whom these certifications <i>shall</i> be submitted. All other contractors should submit a statement of security certification to their CMS POs.	

Table 3.1. Reporting Requirements Planning Table

³ More information about system security planning can be found in the CMS SSP Methodology.

⁴ More information about Risk Assessment Reports can be found in the CMS Information Security Risk Assessment (RA) Methodology.

² NIST defines "significant change" as "any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets."

Requirement	Frequency	Send To	Comments	Complete (check when complete)
3.4 IT Systems Contingency Plan (<i>CP</i>)	CPs <i>shall</i> be reviewed, updated, and certified by management each Federal FY (minimum), or upon significant change. ¹ <i>CPs shall</i> be tested annually.	 SSO CMS CO System Security Profile 	Management and the SSO <i>shall</i> approve the <i>CP</i> . The IT Systems <i>CP</i> is to be developed (in accordance with Appendix B), reviewed, updated, and certified by management— and indicated as such in both the Certification Package/Statement of <i>C</i> ertification and the System Security Profile ⁵ .	
3.5 Compliance	Each Federal FY	 SSO PO CMS CO System Security Profile 	POA&M : POA&Ms address <i>Findings</i> of annual system security assessments including the annual <i>FISMA Evaluation</i> , and, as applicable: SAS 70 audits, CFO controls audits, the Section 912 evaluation, and data center tests and reviews.	
3.6 Incident Reporting and Response	As necessary	POSystem Security Profile	HIPAA also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file with the Principal SSO		

LEGEND:

CFO	Chief Financial Officer
CISS	CMS Integrated Security Suite
CO	Central Office (CMS)
СР	Contingency Plan
CPIC	Certification Package for Internal Controls
FY	Fiscal Year
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
MA	Major Application
PO	Project Officer (CMS)
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SAS	Statement on Auditing Standard
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer
SSP	System Security Plan

NOTE: Documents listed in table 3.1 may be stored as paper documents, electronic documents, or a combination thereof.

When submitting documentation to the CMS Central Office, registered mail or its equivalent (signed receipt required) should be used. For supporting documentation (such as Risk Assessments, Contingency Plans, System Security Plans, etc.), only digital soft copies in the approved CMS format are required. Paper copies are only required for

⁵ More information about contingency planning can be found in An Introduction to Computer Security: The NIST Handbook. SP 800-12, and the Contingency Planning Guide for Information Technology Systems: NIST Special Pub 800-34.

certification signature pages, certifying the completion of required periodic document development, review, updates, and certification. Contact addresses are as follows:

Program Safeguard Contractors (PSCs)

 CMS Central Office Office of Financial Management Program Integrity Group Mail Stop C3-02-16 7500 Security Blvd. Baltimore, MD 21244-1850

Common Working File (CWF) and Shared System Maintainers

 CMS Central Office Office of Information Services Business Application and Management Group Mail Stop N3-13-27 7500 Security Blvd. Baltimore, MD 21244-1850

Fiscal Intermediaries /Carriers/ Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC])

 CMS Central Office Centers for Medicare Management Medicare Contractor Management Group Mail Stop S1-14-17 7500 Security Blvd. Baltimore, MD 21244-1850

Data Centers and Enterprise Data Centers (EDC)

 CMS Central Office Office of Information Services Enterprise Data Center Group Mail Stop N1-19-18 7500 Security Blvd. Baltimore, MD 21244-1850

3.1 System Security Plan (SSP)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The objective of an information security program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process or store Medicare-related data have some level of sensitivity and require protection. The protection of a system *shall* be documented in an *IS* SSP. The completion of an SSP is a requirement of OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law

100-235, the Computer Security Act of 1987. All Medicare claims-related applications and systems categorized as either a Major Application (MA) or General Support System (GSS) *shall* be covered by SSPs.

The purpose of an SSP is to provide an overview of the security requirements of a system and describe the controls that are implemented to meet those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate and cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager (i.e., SSO).

All business partners are required to maintain current SSPs for their Medicare claimsrelated GSSs and MAs in their System Security Profiles. The SSP documents the current level of security within the system or application; that is, actual implemented controls, not planned controls. In addition, the SSP serves as the primary documentation reference for testing and evaluation, whether by CMS, the General Accounting Office (GAO), or other oversight bodies. The SSP is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. Therefore, these security plans should be distributed only on a need-to-know basis.

The SSPs *shall* be available to the SSO and business partner certifying official (normally the VP for Medicare Operations), and authorized external auditors as required. The SSO and *Business* Owner are responsible for reviewing the SSP on an annual basis to ensure that it is up-to-date. The objective of these annual reviews is to verify that the controls selected or installed remain adequate to provide a level of protection to reach an acceptable level of risk to operate the system.

All business partner Medicare claims-related SSPs *shall* be developed in accordance with the most current version of the CMS *Information Security (IS)* System Security Plan (SSP) *Procedures* and the CMS Information Security *Risk Assessment* (RA) and *System Security Plan* (SSP) Guidance, both of which are available on the CMS Web site at: *http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage*. Business partners *shall* also use the most current version of the Microsoft[®] Word[®] SSP template, available at the same Web site.

SSPs *shall* be re-certified within 365 days from the last date certified. The SSP *shall* also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update to the SSP needs to occur. The SSP *shall* be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review and the updated SSP, if applicable, *shall* be placed in the Medicare contractor's System Security Profile, and a copy *shall* be provided to the CMS Central Office.

Contractors updating their current SSP(s) or developing new SSP(s) *shall* include Medicare claims processing front-end, back-end, and/or other claims processing related systems using the most current version of the CMS *Information Security (IS)* System Security Plan (*SSP*) *Guidance*. The CMS *SSP guidance* and template *are available* on the CMS *Web site* at:

http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#TopOfPage.

Front-end systems are those systems Medicare contractors develop and maintain for use in their operations areas and data centers to enter claims and claims-related data into the standard/shared claims processing system. These front-end systems include, but are not limited to: electronic data interchange, imaging systems, optical character recognition, manual claims entry, claims control, provider, beneficiary, other payer databases, and other pre-claims processing business functions. Back-end systems are those systems that Medicare contractors develop and maintain for use in their operations areas and data centers to output claims processing information (i.e., checks, Medicare summary notices, letters, etc). These back-end systems include, but are not limited to: print mail, 1099, post-payment medical reviews, customer service, appeals, overpayment written/phone inquiries and separate claims reconciliation systems.

A newly developed or updated SSP *shall* be sent in electronic form to the CMS Central Office on CD-ROM. This CD-ROM must be received by CMS ten (10) working days after the SSP(s) has been developed, updated, or re-certified. The original signed, dated CMS SSP certification form *shall* be submitted in hard copy along with the electronic CD-ROM copy. This information should <u>not</u> be submitted to the CMS Central Office via email—registered mail or its equivalent (signed receipt required) should be used.

In summary, the SSP *shall* be updated and re-certified annually unless there are changes as discussed above that would necessitate a more frequent update. Should SSP technical assistance be required, direct all questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/Northrop Grumman Help Desk at 703-272-5725.

3.2 Risk Assessment

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners are required to perform an annual risk assessment in accordance with the CMS Information Security *Risk Assessment (IS RA) Procedures* and the CMS Information Security *Risk Assessment (RA)* and *System Security Plan (SSP)* Guidance. These documents are available at *the CMS Web site*: <u>http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage</u>.

The CMS *IS* RA *Procedures* presents a systematic approach for the RA process of Medicare information computer systems within the CMS and business partner environments. The *procedures* describe the steps required to produce an *IS* RA Report for systems and applications that require an SSP. This *procedure* and its resultant report replace the former Triennial RA requirement and report.

All system and information owners *shall* develop, implement, and maintain risk management programs to ensure that appropriate safeguards are taken to protect all CMS resources. A risk-based approach shall be used to determine adequate security and shall include a consideration of the major factors in management such as the value of the system or application, all threats, all vulnerabilities, and the effectiveness of current or proposed safeguards. The CMS *IS* RA *Procedures shall* be used to prepare an annual *IS* RA Report.

All RAs *shall* be re-certified within 365 days from the last date certified. Medicare contractors *shall* review their RA(s) prior to re-certification to determine if an update is needed. An RA *shall* be performed if a significant change to any information system has occurred. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review and/or the updated RA *shall* be placed in the Medicare contractor's System Security Profile. The updated RA(s) *shall* also be mailed to the CMS Central Office. The RA used to support a SSP(s) cannot be dated more than 12 months earlier than the SSP certification date.

Contractors that must update their current RA(s) *shall* use the most current version of the CMS Information Security *Risk Assessment (IS RA) Procedures*. The CMS *procedures* and template *are available* on the CMS Web site at: *http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage*.

A newly developed or updated RA that is submitted with the SSP *shall* be sent to the CMS Central Office on CD-ROM. This CD-ROM must be received by CMS ten (10) working days after they have been developed or updated. This information should <u>not</u> be submitted to the CMS Central Office via email—registered mail or its equivalent (signed receipt required) should be used.

In summary, the RA *shall* be updated annually unless there are changes to either as discussed above that would necessitate a more frequent update. Should RA technical assistance be required, direct all questions to: CyberTyger at CyberTyger@cms.hhs.gov or to the CMS/Northrop Grumman Help Desk at 703-272-5725.

Business partners should refer to the CMS Information Security (*IS*) Acceptable Risk Safeguards (ARS) document to aid in the preparation of a risk assessment. This document *is available on the CMS Web site* at: http://www.cms.hhs.gov/InformationSecurity/70_Guidelines_Tools.asp#TopOfPage.

3.3 Certification

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All Medicare business partners are required to certify their system security compliance. Certification is the formal process by which a contract official verifies, initially and then by annual reassessment, that a system's security features meet CMS CSRs. Business partners *shall* self-certify that their organization(s) successfully completed a security *FISMA Evaluation* of their Medicare IT systems and associated software in accordance with the terms of their Medicare Agreement/Contract.

Each contractor is required to self-certify to CMS its IT systems security compliance within each Federal fiscal year. This security certification *shall* be included in the Certification Package for Internal Controls (CPIC) or, for contracts not required to submit CPIC certifications, send the security certification to their appropriate CMS POs. CMS will continue to require annual, formal re-certification within each fiscal year no later than September 30, including validation at all levels of security as described in this manual.

Systems security certification *shall* be fully documented and maintained in official records. The security certification validates that the following items have been developed (i.e., updated and/or reviewed, as required) and are available for review in the System Security Profile:

- Certification
- FISMA Evaluation (see section 3.5.2 and Appendix A)
- System Security Plan for each GSS and MA (see section 3.1)
- Risk Assessment (see section 3.2)
- IT Systems Contingency Plan (see section 3.4 and Appendix B)
- Plan of Action and Milestones (see section 3.5.3)

3.4 Information Technology (IT) Systems Contingency Plan (*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

All business partners are required to develop and document an IT Systems Contingency Plan that describes the arrangements that have been made and the steps that *shall* be taken to continue IT and system operations in the event of a natural or human-caused disaster. Medicare IT Systems Contingency Plans *shall* be included in management planning and *shall* be:

• Reviewed whenever new systems are planned or new safeguards contemplated

- Reviewed annually to ensure that they remain feasible
- Tested annually. If backup facility testing is done *by Medicare contract type (i.e., when multiple contract types are involved [e.g., Data Center, Part A/B, DMERC])*, each individual Medicare *contract type shall be tested* every year.

Appendix B to this manual provides information on Medicare IT Systems Contingency Plans and testing methods. See Item 3.4 in Table 3.1, section 3.0, for other references.

Each Medicare contractor *shall* review its IT Systems Contingency Plan 365 days from the date it was last reviewed or updated to determine if changes to the contingency plan are needed. A contingency plan should be updated if a significant change has occurred. The system contingency plan *shall* also be tested 365 days from the last test performed. Updated plans and test reports (results) should be placed in the contractor's System Security Profile. Business partner management and the SSO *shall* approve newly developed or updated IT Systems Contingency Plans. Information on Medicare IT systems contingency planning can be found in Appendix B.

A newly developed or updated Medicare IT System Contingency Plan *shall* be submitted to CMS within 10 (ten) working days after the business partner's management and SSO have approved it. A copy of the IT System Contingency Plan *shall* be submitted via CD-ROM to the CMS Central Office along with a hard copy of the statement of certification. This information should not be submitted via email. Registered mail or its equivalent should be used.

3.5.2 Annual FISMA Evaluation (FE) (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A critical factor for maintaining on-going compliance with FISMA and the Federal Managers' Financial Integrity Act of 1982 (FMFIA) is for Business Owners in coordination with developers / maintainers, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing) and person-hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of applicable POA&Ms for vulnerabilities noted during the annual testing.

The purpose of annual FE testing (i.e., validation) is to examine and analyze implemented security safeguards in order to provide evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. The annual FE is intended to validate the security controls to determine the extent to which the controls are:

- *implemented correctly,*
- operating as intended, and
- producing the desired outcome with respect to meeting the security requirements for the system.

To fulfill the annual FE validation obligation, the FE shall be conducted by an independent agent or team. This can be any internal or external agent or team that is capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain of command associated with the information system or to the determination of security control effectiveness.

The annual FE testing requirement has been interpreted by OMB as being within 365 calendar days of the prior test. Over a three (3) year period, all controls applicable to a system or application shall be tested. This means a subset (no less than one-third $[^1/_3]$) of the security controls shall be tested each year so that all controls are tested during a three (3) year period.

While CMS does not mandate which subset of controls should be tested each year or require a specific number of controls to be tested each year, CMS (and OMB) does require that all controls be tested within a three (3) year period. Business Owners, in coordination with the developers / maintainers of CMS applications and systems, are responsible for meeting this requirement.

All management directed testing may be used to meet the requirement for the annual FE testing. Management directed testing includes: independent Security Test and Evaluations (ST&E), testing performed pursuant to CMS compliance with OMB Circular A-123, evaluations and tests conducted under authority of Section 912 of the MMA, Statement on Auditing Standards (SAS) No. 70 internal control reviews, and test results from local test teams organized for purposes of meeting this requirement.

Annual security controls testing, including FE testing, should be used to satisfy the requirements for the ST&E which is an integral component of the CMS Certification and Accreditation (C&A) Program. In order to be considered as part of a system's or application's ST&E, the annual security control testing shall meet the standards for independence.

3.5.3 Plan of Action and Milestones (POA&Ms)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners are required to submit a monthly POA&M package which is due by the 1st of each month. The POA&M package consists of a CISS-generated POA&M data file and, if required by CMS, any additional supporting documentation.

3.5.3.1 Background

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The FISMA requires that Federal agencies provide annual reporting of the state of security programs for all IT systems associated with the agency. Additionally, periodic POA&Ms reporting the status of known security weaknesses for all Federal agency systems *shall* also be submitted to the OMB. This reporting requirement applies to a broader scope of security weaknesses, as it is not limited to weaknesses identified by specific audits and reviews (such as those covered under FMFIA). In the case of FISMA, any security weakness identified for covered systems *shall* be reported and included in a periodic POA&M report.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for both MAC contractors and existing carrier and intermediary business partners (to include their respective data centers). These Section 912 evaluations and reports necessitate an annual on-site review of business partner security programs to ensure that they meet the information security requirements imposed by FISMA. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified deficiencies be addressed in a report to be submitted shortly after the evaluation results are finalized, as well as periodically thereafter to track updated progress towards completion of the identified action plans.

The CISS enables contractors to satisfy reporting requirements for EDP security-related findings. Security-related finding (and approved action plan) data is entered into the CISS following all audits/reviews, from which the CISS generates a single monthly submission data file that summarizes the current state of security for the business partner. This data file is submitted to CMS as part of the monthly POA&M package.

3.5.3.2 POA&M Package Components/Submission Format

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

In addition to the initial POA&M reporting that follows each audit/review, summary POA&Ms shall be submitted on the 1st of each month via the CISS. The CISS shall be populated with EDP security-related findings from the Chief Financial Officer's Electronic Data Processing (CFO EDP) Audit, the Section 912 evaluation, *Data Center ST&E*, the SAS 70 review, the Certification Package of Internal Controls (CPIC), and any other EDP security-related findings that result from an audit or review, whether internal or external. Corrective actions are to be established in the CISS to address all resulting weaknesses entered therein, and those corrective actions *shall* be reflected in the CISS POA&M (both in the data file and reports).

To ensure consistency, all Medicare contractors *shall* enter into the CISS the Section 912 evaluation, Data Center ST&E, and/or CFO EDP Audit POA&Ms that have already been accepted and approved by CMS for its EDP findings, as the standard for all future submitted POA&Ms. Findings from other audits, reviews and evaluations (e.g., SAS 70,

CPIC, internal audits, etc.) that address the same security finding problem should use the same solution (action plan) if it will adequately resolve the identified weakness.

Initial Report. Within 45 days (or as otherwise directed by CMS) of the final results for every internal/external audit/review, an initial, manually generated, CMS POA&M Weakness Tracking Form is due to CMS that describes the findings of the audit/review and initial corrective actions planned for implementation. Upon acceptance from CMS, this information will be entered into the CISS by the Medicare contractor for monthly tracking purposes.

NOTE: Medicare contractors are encouraged to use the draft reports (when available) to prepare their corrective actions for identified findings.

Monthly POA&M Package. On a monthly basis, business partners shall provide updates on progress towards completion of remediation efforts for weaknesses identified from all known sources. The monthly POA&M package shall include a CD-ROM that contains the CISS-generated data file at its root level (refer to the POA&M submission instructions in the CISS User Guide). The naming convention for this file is XXX_POAM(XX-01-200X).mdb where XXX is the acronym for the contractor/*entity*, and the date is the due date of the report.

Medicare contractors *shall* submit the monthly POA&M package to the CMS Central Office (for Title XVIII and MAC contracts) or PO (for FAR contracts). This information should not be submitted via email. Registered mail or its equivalent should be used. A copy *shall* also be placed in the System Security Profile.

3.5.4 Annual/Yearly Compliance Condition

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Many security documents, such as Risk Assessments, SSPs, Contingency Plans, as well as many CMS CSR control techniques (see Appendix A) require annual or yearly performance (e.g., test, submission, recertification, review, update). When such a requirement is to be performed annually or yearly, it is to be performed no later than the one year anniversary date of its previous performance (i.e., within 365 days [366 days in leap years]). The only exceptions to this annual/yearly compliance condition are deliverables whose annual due date are set and distributed by CMS, such as the annual *FISMA Evaluation* submission.

If the *business partner* wishes to change the timing cycle of an annual or yearly requirement compliance date, the *business partner shall* shorten the timing cycle and not lengthen the annual/yearly timing cycle to attain the new performance date. For example, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the *business partner* desired to change the review date to 5/31/07, they would be required to review the SSP no later than 7/31/06 and again no later than 5/31/07, and no later than 5/31/xx thereafter. However, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the *business partner* desired to change the review date to 5/31/07, and no later than 5/31/xx thereafter. However, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the *business partner* desired to change the review date to 9/30/06, they

would be required to review the SSP no later than 7/31/06 and again no later than 9/30/06. The next review cycle would then be no later than 9/30/07 and 9/30/XX thereafter.

3.6 Incident Reporting and Response

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

An incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction.* The business partner *shall* use its security policy and procedures to determine whether the security incident is reportable (as defined below). Upon receiving notification of an IT systems security incident or a suspected incident, the SSO *shall* immediately perform an analysis to determine if an incident actually occurred. The incident could result in adversely impacting the processing of Medicare data or the privacy of Medicare data. Reportable incidents include:

- Unauthorized Disclosure: *Information disclosure with risk to privacy information or public relations impact*
- **Denial of Service:** *A*n attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- Malicious Code: *A* virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- Unauthorized Access: *A* breach in which person gains logical or physical access to network, system application, data or other resource without permission
- **Inappropriate Usage:** *A* violation of acceptable computing use policies
- **Multiple Components:** *A* single incident that encompasses two or more incidents

3.6.1 Computer Security Incident Response

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All suspected information security incidents or events shall be reported to the CMS IT Service Desk (or equivalent business partner function) as soon as an incident comes to the attention of a CMS information or information system user. All confirmed security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS Information Security Incident Handling and Breach Analysis/Notification Procedure. This document is available on the CMS Web site at <u>http://www.cms.hhs.gov/InformationSecurity/15_Procedures.asp#TopOfPage</u>. The CMS IT Service Desk can be contacted by telephone at 410-786-2580 or by e-mail at: cms it service desk~cms.hhs.gov.

All CMS contractors and business partners shall utilize the following incident categories, Table 3.2, and reporting time criteria, Table 3.3, when reporting incidents to CMS.

Category	Name	Description
CAT 0	Exercise /Network Defense Testing	Used during State, Federal, national, international exercises, and approved activity testing of internal/external network defenses or responses.
CAT 1	Unauthorized Access*	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
CAT 2	Denial of Service*	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
CAT 3	Malicious Code*	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
CAT 4	Inappropriate Usage*	A person violates acceptable computing use policies.
CAT 5	Probes and Reconnaissance Scams	This category includes any activity that seeks to access or identify a Federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
PII	Personally Identifiable Information (PII) Exposure	Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual.

 Table 3.2. Incident Categories

*Source: NIST SP 800-61

Category	Reporting Timeframe	
CAT 0	Not applicable; this category is for CMS' internal use during exercises.	
CAT 1	Within one (1) hour of discovery /detection.	
CAT 2	Within two (2) hours of discovery /detection if the successful attack is still	
	ongoing and the agency is unable to successfully mitigate activity.	
CAT 3	Daily; within one (1) hour of discovery /detection if widespread across	
	agency.	
CAT 4	Weekly.	
CAT 5	Not applicable; this category is for classified systems.	
CAT 6	Not applicable; this category is for CMS' use to categorize a potential	
	incident that is currently being investigated.	
PII	Within one (1) hour of discovery /detection.	

Table 3.3. Incident Reporting Timeframe Criteria

When reporting confirmed security incidents, business partners should report the date and time when events occurred or were discovered; names of systems, programs, or networks effected by the incident; and impact analysis. Release of information during incident handling *shall* be on an as-needed and need-to-know basis. When other entities should be notified of incidents at external business partner sites, CMS will coordinate with legal and public affairs contacts at the effected entities. If a violation of the law is suspected, CMS will notify the Office of the Inspector General's (OIG) Computer Crime Unit and submit a report to the FedCIRC of the incident with a copy to the CMS Senior Information Systems Security Office.

As part of the risk management process, the business partner should determine the extent of the incident's impact and the potential for new or enhanced controls required to mitigate newly identified threats. These new security controls (and associated threats and impacts) should provide additional input into the business partner's risk assessment. Business partners should refer to The CMS *Information* Security Incident Handling *and Breach Analysis/Notification* Procedure for further guidance.

3.7 System Security Profile

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Consolidate security documentation (paper documents, electronic documents, or a combination) into a System Security Profile that includes the following items:

- Completed FISMA Evaluation
- System Security Plan (for each GSS and MA)
- Risk Assessments
- Certifications

- IT Systems Contingency Plans
- POA&Ms for each compliance security review
- POA&Ms for other security review undertaken by HHS OIG, CMS, IRS, GAO, consultants, subcontractors, and business partner security staff
- Incident reporting and responses
- Systems security policies and procedures

The System Security Profile shall be kept in a secure location, kept up-to-date, and pointers to other relevant documents maintained. A backup copy of the System Security Profile shall be kept at a secure off-site storage location, preferably at the site where back-up tapes and/or back-up facilities are located. The back-up copy of the profile shall also be kept up-to-date, particularly the contingency plan documents.

3.10.1 Security Configuration Management

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires NIST to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal government.

CMS security configuration management guidance, including DHHS requirements and links to NIST, NSA, and DISA configuration guides are provided in Appendix F.

CMS does not require the verbatim use of these guidance documents and tools for the configuration of Medicare systems. However, CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity. CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

NOTE: DMEMACs, ABMACs, and EDCs are required to start with these Security Technical Implementation Guide (STIG) baseline configurations and then document any exceptions based on environment specific implementation.

3.10.2 National Institute of Standards and Technology (NIST)

(*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

CMS, as a government agency, highly encourages business partners to review and incorporate the NIST concepts into their Medicare security program. Under the Computer

Security Act of 1987 (P.L. 100-235), NIST develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on IT security issues. The publications are issued as Federal Information Processing Standards Publications (FIPS), Special Publications (SP), NIST Interagency Reports (NISTIRs), and IT Laboratory (ITL) Bulletins.

Special Publications in the 800 series (SP 800-XX) present documents of general interest to the computer security community. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (P.L. 104-106) and the Computer Security Act of 1987 (P.L. 100-235). With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, references to the "waiver process" contained in many of the FIPS are no longer operative. Note, however, that not all FIPS are mandatory; consult the applicability section of each FIPS for details.

CMS does not normally require the verbatim use of NIST SPs for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are *specified* in the CMS BPSSM and the CMS CSRs. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop security standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

Table 3.4 contains a listing of NIST publications relevant to common systems or technology utilized within the Medicare business partner community. Table 3.4 is not meant to be all-inclusive and may contain some references that are not applicable to a particular Medicare business partner application. The most current NIST publications *are available* at: <u>http://csrc.nist.gov/publications/index.html</u>.

Publication Number	Title
SP 800-113 (Draft)	Guide to SSL VPNs
SP 800-111 (Draft)	Guide to Storage Encryption Technologies for End User
	Devices
SP 800-110 (Draft)	Information System Security Reference Data Model
SP 800-103 (Draft)	An Ontology of Identity Credentials, Part I: Background and
	Formulation
SP 800-101	Guidelines on Cell Phone Forensics
SP 800-100	Information Security Handbook: A Guide for Managers
SP 800-98	<i>Guidelines</i> for Securing Radio Frequency Identification (RFID)
	Systems

Table 3.4. NIST Publications

Publication Number	Title	
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to	
	IEEE 802.11i	
SP 800-96	Personal Identity Verification (PIV) Card / Reader	
	Interoperability Guidelines	
SP 800-95	Guide to Secure Web Services	
SP 800-94	Guide to Intrusion Detection and Prevention Systems (<i>IDPS</i>)	
SP 800-92	Guide to Computer Security Log Management	
SP 800-89	Recommendation for Obtaining Assurances for Digital	
	Signature Applications	
SP 800-88	Guidelines for Media Sanitization	
SP 800-86	Guide to <i>Integrating</i> Forensic Techniques <i>in</i> to Incident	
	Response	
SP 800-85A	PIV Card Application and Middleware Interface Test	
	Guidelines	
SP 800-85B	PIV Data Model Conformance Test Guidelines	
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans	
	and Capabilities	
SP 800-83	Guide to Malware Incident Prevention and Handling	
SP 800-82 (Draft)	Guide to Industrial Control Systems (ICS) Security	
SP 800-81	Secure Domain Name System (DNS) Deployment Guide	
SP 800-80 (Draft)	Guide for Developing Performance Metrics for Information	
	Security	
SP 800-79	Guidelines for the C&A of PIV Card Issuing Organizations	
SP 800-78 <i>Rev. 1</i>	Cryptographic Standards and Key Sizes for PIV	
SP 800-77	Guide to IPsec VPNs	
SP 800-76 <i>Rev.</i> 1	Biometric Data Specification for PIV	
SP 800-73 Rev. 2	Interfaces for PIV (4 parts): 1- Card Application Namespace,	
	Data Model & Representation 2- Card Appl. Card Command	
	Interface 3- Client Appl. Programming Interface 4-	
	Transitional Interfaces & Data Model	
SP 800-72	Guidelines on PDA Forensics	
SP 800-70	Security Configuration Checklists Program for IT Products:	
	Guidance for Checklists Users and Developers	
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT	
	Professionals: A NIST Security Configuration Checklist	
SP 800-67	Recommendation for the Triple Data Encryption Algorithm	
	(TDEA) Block Cipher	
SP 800-66	An Introductory Resource Guide for Implementing the Health	
	Insurance Portability and Accountability Act (HIPAA) Security	
	Rule	
SP 800-65	Integrating Security into the Capital Planning and Investment	
	Control Process	

Publication Number	Title	
SP 800-64 Rev. 1	Security Considerations in the Information System	
	Development Life Cycle	
SP 800-63 Ver. 1.0.2	Electronic Authentication Guideline: Recommendations of the	
	NIST	
SP 800-61 <i>Rev. 1</i>	Computer Security Incident Handling Guide	
SP 800-60 Vols. 1&2	Guide for Mapping Types of Information and Information Systems to Security Categories	
SP 800-59	Guideline for Identifying an Information System as a National	
SP 800-58	Security System	
	Security Considerations for Voice Over IP (VoIP) Systems	
SP 800-57	Recommendation <i>for</i> Key Management	
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	
SP 800-55 <i>Rev. 1</i>	Performance Measurement Guide for Information Security	
(Draft)		
SP 800-54	Border Gateway Protocol Security	
SP 800-53A (Final	Guide for Assessing the Security Controls in Federal	
Draft)	Information Systems	
SP 800-53 Rev. 2	Recommended Security Controls for Federal Information	
	Systems	
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE)	
	Vulnerability Naming Scheme	
SP 800-50	Building an IT Security Awareness and Training Program	
SP 800-49	Federal S/MIME V3 Client Profile	
SP 800-48 <i>Rev.</i> 1	Wireless Network Security <i>for IEEE</i> 802.11 <i>a/b/g and</i>	
(Draft)	Bluetooth	
SP 800-47	Security Guide for Interconnecting IT Systems	
SP 800-46, Ver. 2	User's Guide to Securing External Devices for Telework and	
(Draft)	Remote Access	
SP 800-45 Ver. 2	Guidelines on Electronic Mail Security	
SP 800-44 Ver. 2	Guidelines on Securing Public Web Servers	
SP 800-43	Systems Administration Guidance for Windows 2000 Professional	
SP 800-42	Guideline on Network Security Testing	
SP 800-41	Guidelines on Firewalls and Firewall Policy	
SP 800-40 Ver. 2	Creating a Patch and Vulnerability Management Program	
SP 800-37	Guide for the Security C&A of Federal Information Systems	
SP 800-36	Guide to Selecting <i>IT</i> Security Products	
SP 800-35	Guide to IT Security Services	
SP 800-34	Contingency Planning Guide for IT Systems	
SP 800-33	Underlying Technical Models for IT Security	
SP 800-32	Introduction to Public Key Technology and the Federal PKI	
	Infrastructure	

Publication Number	Title	
SP 800-30	Risk Management Guide for IT Systems	
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2	
SP 800-28 Ver. 2 (Draft)	Guidelines on Active Content and Mobile Code	
SP 800-27 Rev. A	Engineering Principles for IT Security (A Baseline for Achieving Security)	
SP 800-26 Rev. 1	Guide for Information Security Program Assessments and System Reporting Form WITHDRAWN	
SP 800-25	Federal Agency Use of <i>Public Key Technology</i> for Digital Signatures and Authentication	
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does	
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products	
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications	
SP 800-21 <i>Rev.</i> 1	2 nd Edition, Guideline for Implementing Cryptography in the Federal Government	
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures	
SP 800-19	Mobile Agent Security	
SP 800-18 Rev. 1	Guide for Developing Security Plans for <i>Federal</i> IT Systems	
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures	
SP 800-16	IT Security Training Requirements: A Role- and Performance- Based Model	
SP 800-15 Ver. 1	Minimum Interoperability Specification for PKI Components (MISPC)	
SP 800-14	Generally Accepted Principles and Practices for Securing IT Systems	
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network	
SP 800-12	An Introduction to Computer Security: The NIST Handbook	
FIPS 201-1	Personal Identity Verification (PIV) for Federal Employees and Contractors	
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems	
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems	
FIPS 198-1 (Draft)	The Keyed-Hash Message Authentication Code (HMAC)	
FIPS 197	Advanced Encryption Standard	

Publication Number	Title	
FIPS 196	Entity Authentication Using Public Key Cryptography	
FIPS 191	Guideline for <i>the</i> Analysis of LAN Security	
FIPS 190	Guideline for the Use of Advanced Authentication Technology	
	Alternatives	
FIPS 188	Standard Security Labels for Information Transfer	
FIPS 186-3 (Draft)	Digital Signature Standard (DSS)	
FIPS 185	Escrowed Encryption Standard	
FIPS 181	Automated Password Generator	
FIPS 180-3 (Draft)	Secure Hash Standard (SHS)	
FIPS 140-3 (Draft)	Security Requirements for Cryptographic Modules	
FIPS 113	Computer Data Authentication	

CMS continues to work closely with NIST in the development of new standards, FIPS, and security documentation to ensure the highest and most reasonable level of security of Medicare data.

4.1 Security Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FISMA defines three security objectives for information and information systems: confidentiality, integrity, and availability (CIA). FISMA also directs the promulgation of Federal standards for: (i) the security categorization of Federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category. These Federal standards are issued in the form of FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, respectively.

With the passage of FISMA, there is no longer a provision that allows agencies to waive mandatory Federal Information Processing Standards (FIPS). This waiver provision was included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, any references to a "waiver process" contained in any existing FIPS Pub is no longer valid. In addition, OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management, states that government contractors shall abide by FISMA requirements and each agency shall ensure their contractors are doing so.

4.1.1 Potential Security Impact Levels

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FIPS Pub 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or

availability). The application of these definitions shall take place within the context of each organization and the overall national interest.

Table 4.1 defines the three system security levels and their potential security impact.

Security Level	Result	Explanation	
High (H)	Catastrophic Adverse Effect	 Severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; Major damage to organizational assets; Major financial loss; or Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. 	
Moderate (M)	Serious Adverse Effect	 Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; Significant damage to organizational assets; Significant financial loss; or Significant harm to individuals that does not involve loss of life or serious life threatening injuries. 	
Low (L)	Limited Adverse Effect	 Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; Minor damage to organizational assets; Minor financial loss; or Minor harm to individuals. 	

Table 4.1. System Security Level Definitions

4.1.2 Security Levels by Information Type (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS categorized its information according to information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

CMS has defined eleven information types processed by CMS information systems (see Table 4.2 below). For each information type, CMS used FIPS Pub 199 to determine its associated security category by evaluating the potential impact value (e.g., High, Moderate, or Low) for each of the three FISMA security objectives—CIA. The resultant security categorization is the CMS System Security Level. This is the basis for assessing the risks to CMS operations and assets, and in selecting the appropriate minimum security controls and techniques (i.e., CSRs).

The generalized format for expressing the security category (SC) of an information system is:

SC information system = {(confidentiality impact), (integrity impact), (availability impact)},

where the acceptable values for potential impact are High, Moderate, or Low.

Table 4.2 lists the FIPS Pub 199 security levels for the various information types. The system security level for a FISMA system or application system is determined by its information type(s).

NOTE: In cases where information of varying security levels is combined in a FISMA system or application, the highest security level takes precedence.

Information	Explanation and Examples	System Security Level	
Types		Security Categorization (SC)	
Investigation,	Information related to investigations for law enforcement purposes; intelligence-related information that cannot be	HIGH	
intelligence- related, and security information (14 CFR PART 191.5(D))	classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.	SC={(confidentiality, H), (integrity, H), (availability, M)}	
	Information and associated infrastructure directly involved in making payments for Medicare Fee-for-Service (FFS), Medicaid and State Children's Health Insurance Program (SCHIP).	HIGH	
Mission-critical information		SC={(confidentiality, H), (integrity, H), (availability, H)}	
	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974	MODERATE	
Information about persons	(e.g., salary data, social security information, passwords, user identifiers (IDs), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).	SC={(confidentiality, M), (integrity, M), (availability, M)}	

Table 4.2. FIPS 199 Security Levels by Information Type

Information	Emporation and Examples	System Security Level Security Categorization (SC)	
Types	Explanation and Examples		
Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payments, payroll, automated decision making, procurement, market-sensitive, inventory, other financially- related systems, and site operating and security expenditures.	MODERATE SC={(confidentiality, M), (integrity, M), (availability, M)}	
Internal administration	Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, advance information concerning procurement actions, management reporting, etc.	MODERATE SC={(confidentiality, M), (integrity, M), (availability, M)}	
Other Federal agency information	Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency.	MODERATE SC={(confidentiality, M), (integrity, M), (availability, L)}	
New technology or controlled scientific information	Information related to new technology; scientific information that is prohibited from disclosure or that may require an export license from the Department of State and/or the Department of Commerce.	MODERATE SC={(confidentiality, M), (integrity, M), (availability, L)}	
Operational information	Information that requires protection during operations; usually time-critical information.	(availability, 2)) MODERATE SC={(confidentiality, M), (integrity, M), (availability, M)}	
System configuration management information	Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information.	MODERATE SC={(confidentiality, M), (integrity, M), (availability, M)}	
Other sensitive information	Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.	<i>LOW</i> SC={(confidentiality, L), (integrity, L), (availability, L)}	
Public information	Any information that is declared for public consumption by official authorities and has no identified requirement for integrity or availability. This includes information contained in press releases approved by the Office of Public Affairs or other official sources.	LOW SC={(confidentiality, L), (integrity, L), (availability, L)}	

4.1.3 CMS Security Level Designation—HIGH (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Although the confidentiality and integrity of some information types (i.e., security category) processed, stored, and/or transmitted on CMS business partner and data center systems could be considered to be at a "Moderate" security level based on the Table 4.2 explanations and examples, CMS has designated all Medicare claims-related information to be "Mission-critical information." Consequently, all CMS business partner and data center information systems shall be designated at a "HIGH" system security level.

Business partner System Managers and System Maintainers/Developers *shall* ensure that their *Medicare claims-related information and information* systems are accessed only by authorized users. The business partner managers of compartmentalized systems *shall* take special care to specify the appropriate level of security required when negotiating with GSSs and MAs for services. The *"HIGH"* security level designation determines the minimum security safeguards required to protect sensitive data and to ensure the operational continuity of *mission*-critical data processing capabilities.

The "HIGH" security level designation applies to both user information and system information, and it is applicable to information in *both digital and* non-*digital* form. System information (e.g., network routing tables, password files, and cryptographic key management information) *shall* be protected at the same level to ensure information and information system confidentiality, integrity, and availability.

4.1.4 Minimum System Security Requirements—HIGH (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FIPS Pub 200 specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. To comply with FIPS Pub 200, agencies shall first determine the security category (i.e., information type) of their information system in accordance with the provisions of FIPS Pub 199, and then apply the appropriate set of baseline security controls contained in NIST SP 800-53 (as amended), Recommended Security Controls for Federal Information Systems. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in NIST SP 800-53. This allows agencies, such as CMS, to adjust the security controls to more closely fit its mission requirements and operational environments.

The CMS Policy for the Information Security Program (PISP) individual policy statements, along with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) required security standards provide technical guidance to CMS and its contractors as to the minimum level of security controls that shall be implemented to protect CMS's information and information systems. These two CMS documents, along with other Federal requirements, form the basis for the CISS CSRs.

4.2 Sensitive Information Protection Requirements

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Business partners are responsible for implementing *the* Minimum Protection Standards (MPS) for all *CMS sensitive* information (*digital and non-digital*) and information systems categorized at *the* "HIGH" security level designation. The MPS establishes a uniform method for protecting data and items that require safeguarding. The MPS applies to all IT facilities, areas, or systems processing, storing, or transmitting CMS sensitive information (*i.e., any information categorized as "HIGH"*) in any form or on any media.

The following table should be used to determine the minimum standards required to protect CMS sensitive information. Note that any of the three alternative protection standards is acceptable whenever all of the applicable perimeter, interior area, and/or container standards are met. The following alternative methods are not listed in any order of preference or security significance.

	Perimeter Type	Interior Type	Container Type
Alternative #1	Secured		Locked
Alternative #2	Locked	Secured	
Alternative #3	Locked		Security

 Table 4.3. MPS Physical Security

Because local factors may require additional security measures, management *shall* analyze local circumstances to determine space, container, and other security needs at individual facilities. The MPS has been designed to provide management with a basic framework of minimum security requirements.

The objective of these standards is to prevent unauthorized access to CMS sensitive information. MPS requires two barriers to accessing sensitive information under normal security (*see Table 4.3*).

"Locked" means a perimeter, area, or container that has both a lock and keys or combinations that are controlled. A secured container is a lockable metal container with a resistance to forced penetration, with both a security lock and keys or combinations that are controlled. (See the following sections for additional explanation and details on these requirements.)

The reason for the two barriers is to provide an additional layer of protection to deter, delay, or detect surreptitious entry. Protected information *shall* be containerized in areas where other than authorized employees may have access after hours (e.g., security personnel or custodial service personnel).

4.2.1 Restricted Area

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A restricted area is a secured area whose entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas *shall* either meet secured area criteria or provisions *shall* be made to store CMS sensitive items in appropriate containers during non-working hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information.

Restricted areas *shall* be indicated by prominently posted signs and separated from nonrestricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and each entrance *shall* have controlled access (*e.g.*, electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by a responsible employee positioned at the entrance to enforce the restriction of access to authorized personnel accompanied by one or more officials.

4.2.2 Security Room

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A security room is a room that has been constructed to resist forced entry. The primary purpose of a security room is to store protectable material. The entire room *shall* be enclosed by slab-to-slab walls constructed of approved materials (*e.g.*, masonry brick, dry wall, etc.) and supplemented by periodic inspection. All doors for entering the security room *shall* be locked with locking systems meeting the requirements set forth below (section 4.2.5, Locking Systems). *Entry is limited to specifically authorized personnel*.

Door hinge pins shall be non-removable or installed on the inside of the room. Additionally, any glass in doors or walls *shall* be security glass (*a minimum of* two layers of 1/8-inch plate glass with .060-inch [1/32] vinyl interlayer, nominal thickness shall be 5/16-inch). Plastic glazing material is not acceptable. Vents and louvers *shall* be protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciates at a protection console, UL-approved central station, or local police station; *and the IDS shall* be given top priority for guard/police response during any alarm situation.

Cleaning and maintenance should be performed in the presence of an employee authorized to enter the room.

4.2.3 Secured Areas (Secured Interior / Secured Perimeter) (*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

Secured areas are *interior or exterior perimeters which* have been designed to prevent undetected entry by unauthorized persons during non-working hours. To qualify as a *secured* area, the *area shall* meet the following minimum standards:

- Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, or any lesser-type partition supplemented by UL-approved electronic IDS and fire detection systems.
- Unless electronic IDS devices are used, all doors entering the space *shall* be locked and strict key or combination control should be exercised.
- In the case of a fence and gate, the fence *shall* have IDS devices or be continually guarded, and the gate *shall* be either guarded or locked with intrusion alarms.
- The space *shall* be cleaned during working hours in the presence of a regularly assigned employee.

4.2.4 Containers

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving, desk and credenza drawers, carts, *or* any other piece of office equipment designed for the storage of files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide any protection value (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.2.4.1 Locked Container

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A lockable container is a commercially available or prefabricated metal cabinet or box with riveted or welded seams, or metal desks with lockable drawers. The lock mechanism may be either a built-in key, or a hasp and lock.

4.2.4.2 Security Container

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks should have only two keys and strict control of the keys is mandatory. *If combinations are used, they shall* be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files.
- Metal lateral files equipped with lock bars on both sides and secured with security padlocks.

- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks.
- Key lock "Mini Safes" properly mounted with appropriate key control.

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

4.2.4.3 Safes/Vaults

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A safe/vault is not required for storage of CMS sensitive information. However, if used, *they shall* meet the following requirements:

- A safe is a GSA-approved container of Class *I*, IV, or V, or UL listings of TRTL-30 or TRTL-60.
- A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings that uses UL-approved vault doors and meets GSA specifications.

4.2.5 Locking Systems

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Minimum requirements for locking systems for secured *a*reas and security *r*ooms are high-security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted deadbolt lock.
- Have a deadbolt throw of one (1) inch or longer.
- Double-cylinder design. Cylinders have five (5) or more pin tumblers.
- Contains hardened inserts or inserts made of steel if bolt is visible when locked.
- Both *the* key and lock *shall* be "off-master."

Convenience-type locking devices such as card keys, sequenced button-activated locks used in conjunction with electric strikes, etc., are authorized for use only during working hours. Keys to secured areas not in the personal custody of an authorized employee and *any* combinations *shall* be stored in a security container. *The number of keys or persons with knowledge of the combination to a secured area shall be kept to a minimum.*

4.2.6 Intrusion Detection Systems (IDS)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Physical Intrusion Detection Systems are designed to detect attempted *breaches of* perimeter areas. Physical IDS devices can be used in conjunction with other measures to provide forced entry protection *for* non-working hour *security*. Additionally, alarms for individual and document safety (fire), and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical IDS devices include, but are not limited to: door and window contacts, magnetic switches, motion detectors, and sound detectors, *that* are designed to set off an alarm at a given location when the sensor is disturbed.

5.0 Internet Security

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Transmission of and/or receipt of health care transactions (claims, remittances, etc.) or other CMS sensitive data over the Internet is prohibited at Medicare business partners (or their agents). Practically, this prohibition means that CMS requires the use of private networks or dial-up connections with any entity that transmits or receives health care transactions and/or CMS sensitive data to or from the Medicare contractor. CMS is closely following the health care industry's movement toward adoption of industry-wide security technologies that ensure confidentiality, integrity, and availability of data moved over the Internet and will reconsider its policy at the appropriate time.

Business Partners may use the Internet for: 1) utilizing the IRS Filing Information Returns (FIRE) system by Medicare contractors for Form 1099 submissions, and 2) utilizing e-mail to transmit sensitive information via encrypted attachments in accordance with all applicable CSRs. If not already emplaced, contractors must install firewalls, filtering technology to screen incoming email for high risk transmissions such as executables, up-to-date virus protection software, and intrusion detection software to utilize the Internet.

Appendix A: The CMS Integrated Security Suite (CISS) and the CMS Core Security Requirements (CSRs)

Table of Contents

(Rev. 9, 06-20-08)

1 Introduction to the CMS Integrated Security Suite (CISS)

2 CISS *FISMA Evaluation* Module

- 2.1 Applicable Laws
- 2.2 CMS CSR Security Controls
 - 2.2.1 Security Categorization and Impact Level
 - 2.2.2 Baseline and Enhancement Security Controls
- 2.3 CSR *Security Control* Elements
 - 2.3.1 CSR Attachments and Assessment Impact Levels
 - 2.3.2 Security Control Family, Identifier, and Class
 - 2.3.3 Baseline and Enhancement Control Number and Name
 - 2.3.4 Control
 - 2.3.5 Guidance
 - 2.3.6 Applicability
 - 2.3.7 References
 - 2.3.8 Related Controls
 - 2.3.9 Assessment Procedures
 - 2.3.9.1 Assessment Objective
 - 2.3.9.2 Assessment Methods and Objects
- 2.4 Completing the *FISMA Evaluation*
 - 2.4.1 FISMA Evaluation Control Selection
 - 2.4.2 Security Control Assessment
- 2.5 All *CSR* Responses
- 2.6 "Not Applicable" (N/A) Response Status
- 2.7 *Compliance Status*
 - 2.7.1 *"Met"* Response Status
 - 2.7.2 "Not Met" Response Status
- 2.8 Findings and Weaknesses
 - 2.8.1 Findings
 - 2.8.1.1 Finding Identifier
 - 2.8.1.2 Finding Title and Description
 - 2.8.1.3 Finding Status
 - 2.8.1.4 Determination of Finding Risk Level
 - 2.8.1.5 Finding FMFIA and CPIC Severity
 - 2.8.1.6 Finding *Security Control Family*
 - 2.8.1.7 Finding Point(s) of Contact
 - 2.8.2 Weaknesses
 - 2.8.2.1 Weakness Identifier
 - 2.8.2.2 Weakness Title and Description
 - 2.8.2.3 Weakness *Security Control Family*

- 2.8.2.4 Determination of Weakness Risk Level
- 2.8.2.5 Weakness FISMA Severity
- 2.8.2.6 Weakness Type
- 2.8.2.7 Weakness Status
- 2.8.2.8 Weakness Point(s) of Contact
- 2.8.2.9 Determining Risk
 - 2.8.2.9.1 Likelihood of Occurrence
 - 2.8.2.9.2 Impact Severity
 - 2.8.2.9.3 *Determining the* Risk *Level*
- 2.9 Action Plans and POA&Ms
 - 2.9.1 Completing Action Plans
 - 2.9.1.1 Action Plan Title and Description
 - 2.9.1.2 Determining Completion Dates
 - 2.9.1.3 Determining Costs
 - 2.9.1.4 Determining Funding Sources
 - 2.9.1.5 Milestone Title and Description
 - 2.9.1.6 Milestones with Completion Dates
 - 2.9.1.7 Milestone Changes

(*Rev. 9*)

Attachments:

- 1 CMS Core Security Requirements (CSR) for High Impact Level Assessments
- 2 CMS Core Security Requirements (CSR) for Moderate Impact Level Assessments
- 3 CMS Core Security Requirements (CSR) for Low Impact Level Assessments

1 Introduction to the CMS Integrated Security Suite (CISS)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This appendix applies to CMS Business Partners and all other CMS internal/external organizations directed by CMS to use the CISS. CMS Business Partners and other entities are required by CMS to use the CISS to report the status of Federally- and CMS-mandated security objectives. All CMS-approved Findings from internal or external audits or Federal Information Security Management Act (FISMA) Evaluations shall be entered into the CISS. From these Finding entries, Weakness and Action Plan entries shall be generated and linked with other CISS data as appropriate. This information becomes part of the monthly Plan of Action and Milestones (POA&M) package as directed in section 3.5.3 of the BPSSM.

The term "organization" in this appendix applies to all CMS Business Partners and all CMS internal/external information system Business Owners, contractors, sub-

contractors, entities, and their respective employees and facilities supporting CMS business missions.

The mechanics of CISS use are provided in the CISS User Guide, while guidance for populating specific fields is provided in this appendix. The CISS is available for download on the CMS Web site.

2 CISS *FISMA Evaluation* Module

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The annual FISMA Evaluation of controls module functions in conjunction with the normal Audit/POA&M reporting/tracking process within the CISS. For the Annual FISMA Evaluation, organizations enter text responses to a subset of the full CMS Core Security Requirements (CSR)—see Attachment A—indicating the organization's status towards compliance with CMS security requirements. In this manner, CMS organizations are able to perform their required annual systems security FISMA Evaluations.

The CISS also assists *organizations* by validating and preparing the *FISMA Evaluation* data file for submission to CMS as part of its annual certification material. The CISS *FISMA Evaluation* module provides *organizations* with a powerful reporting tool that generates formatted *FISMA Evaluation* forms, copies of CMS CSRs, and standardized reports.

Organizations shall complete the CISS *FISMA Evaluation* and submit a separate copy for each contract type (i.e. data center, fiscal intermediary, carrier, program safeguard contractor, standard system maintainer, Medicare Administrative Contractor, coordination of benefits, etc.) on CD-ROM to both the CMS Central Office and the Consortium Contractor Management Officer (CCMO) for Title XVIII contracts or the Project Officer (PO) for Federal Acquisition Regulation (FAR) contracts by close of business *on the last business day of* April, *each calendar year except for 2008 when the CISS is due by close of business on August 1, 2008*. This information *may* not be submitted to CMS via email. *Instead*, Registered Mail[™] or its equivalent *shall* be used. *If* technical assistance *is needed*, contact the CMS/Northrop Grumman Help Desk at 703-272-5725.

The completed *Annual FISMA Evaluation shall* be included in the *organization's* Security Profile (see section 3.7 of the BPSSM). *Organizations* may also use the CISS to conduct *reviews* in preparation for audits by specific external entities such as the Government Accounting Office (GAO), Internal Revenue Service (IRS), Department of Health and Human Services (HHS) Office of Inspector General (OIG), and CMS. The CISS *enables organizations* to generate a worksheet consisting of those CSRs and Protocols that have a particular source document as a reference (e.g., IRS Pub 1075, NIST, FISCAM, etc.).

Instructions for using the CISS are contained in the CISS User Guide, which is available in the application itself by clicking on the Help link at the top of the main menu.

2.1 Applicable Laws

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS CSRs detail technical requirements for CMS *organizations that* use information systems to process Medicare data. *Organizations shall* establish and maintain responsible and appropriate controls to ensure the confidentiality, integrity, and availability of Medicare data.

The CMS CSRs are developed by assessing and analyzing requirement statements from a number of Federal and CMS mandates, including the following:

- Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004. http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html
- OMB Circular No. A-127, Financial Management Systems, June 21, 1995. http://www.whitehouse.gov/omb/circulars/index.html
- OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999. <u>http://www.whitehouse.gov/omb/circulars/a127transmittal2.html</u>
- OMB Circular No. A-127, Financial Management Systems, Transmittal 3, December 1, 2004. http://www.whitehouse.gov/omb/memoranda/fy2005/m05-02.html
- OMB Circular No. A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000. <u>http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html</u>
- Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000. <u>http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html</u>
- Health Insurance Portability and Accountability Act (HIPAA), August 21, 1996. <u>http://aspe.os.dhhs.gov/admnsimp/pl104191.htm</u> <u>http://aspe.os.dhhs.gov/admnsimp/nprm/sec13.htm</u>
- Federal Information Security Management Act of 2002 (FISMA), November 27, 2002.
 <u>http://csrc.nist.gov/drivers/documents/FISMA-final.pdf</u>

- Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources, Memorandum, July 17, 2004. <u>http://www.whitehouse.gov/omb/memoranda/fy04/m-04-15.pdf</u>
- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, January 1999. <u>http://www.gao.gov/special.pubs/12_19_6.pdf</u>
- NIST Special Publication 800-53 *Revision 2*, Recommended Security Controls for Federal Information Systems, *December 2007*. <u>http://www.csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2final.pdf</u>
- NIST Special Publication 800-53A Final Public Draft, Guide for Assessing the Security Controls in Federal Information Systems, December 2007. <u>http://www.csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-A</u>
- CMS Information Security (IS) System Security Plans (SSP) Procedures, Version 4.0 Draft, July 10, 2007. <u>http://www.cms.hhs.gov/InformationSecurity</u>
- CMS Information Security Risk Assessment (IS RA) Procedures, Version 4.0 Draft, July 23, 2007. <u>http://www.cms.hhs.gov/InformationSecurity/Downloads/TBD</u>
- CMS Policy for the Information Security Program (PISP), CMS-CIO-POL-SEC02-02, November 15, 2007. <u>http://www.cms.hhs.gov/InformationSecurity/Downloads/PISP.pdf</u>
- CMS Information Security (IS) Acceptable Risk Safeguards (ARS), Version 3.0, September 19, 2007. <u>http://www.cms.hhs.gov/InformationSecurity/Downloads/ARS.pdf</u>
- Tax Information Security Guidelines for Federal, State and Local Agencies and Entities, February 2007. <u>http://www.irs.gov/pub/irs-pdf/p1075.pdf</u>

2.2 CMS CSR Security Controls (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS CSRs comply with the CMS Policy for Information Security Program (PISP) approach by providing a defense-in-depth security structure along with a least-privilege approach and a need-to-know basis for all information access. The CSRs are not intended to be an all-inclusive list of security controls and are subject to regular updates

to reflect the changing technological environment. The CSRs are not intended to replace a Business Owner's due diligence to incorporate controls to mitigate risk. These controls are the minimum to be considered throughout the risk management process and the System Development Life Cycle (SDLC), and employed where applicable.

The Business Owner, system developer/maintainer, and other internal/external organizations directed by CMS are the target audience for the CSRs. They have primary responsibility for determining the information security requirements and ensuring their implementation. Any organization involved in the SDLC could use this information to understand the baseline information security protections required by CMS.

The CMS CSR security controls in the CISS have a well-defined organization and structure. The security controls are organized into seventeen (17) security control families for ease of use in the control selection and specification process. The security controls in each family are related by their functionality.

The 17 security control families are established by NIST SP 800-53 (as amended), Recommended Security Controls for Federal Information Systems. These security control families are aligned closely with the 17 security-related areas specified in FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

A two-character identifier is assigned to uniquely identify each security control family. Table A-1 summarizes the security control families and the two-character identifier used in the CMS CSRs:

Family / Identifier	Description
Access Control (AC)	The standards listed in this section focus on how the organization shall limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
Awareness and Training (AT)	The standards listed in this section focus on how the organization shall: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
Audit and Accountability (AU)	The standards listed in this section focus on how the organization shall: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Table A-1. CSR Security Control Family Descriptions

Family / Identifier	Description
Certification, Accreditation, and Security Assessments (CA)	The standards listed in this section focus on how the organization shall: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Configuration Management (CM)	The standards listed in this section focus on how the organization shall: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.
Contingency Planning (CP)	The standards listed in this section focus on how the organization shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Identification and Authentication (IA)	The standards listed in this section focus on how the organization shall identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Incident Response (IR)	The standards listed in this section focus on how the organization shall: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
Maintenance (MA)	The standards listed in this section focus on how the organization shall: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Media Protection (MP)	The standards listed in this section focus on how the organization shall: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.
Physical and Environmental Protection (PE)	The standards listed in this section focus on how the organization shall: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Family / Identifier	Description	
Planning (PL)	The standards listed in this section focus on how the organization shall develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.	
Personnel Security (PS)	The standards listed in this section focus on how the organization shall: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.	
Risk Assessment (RA)	The standards listed in this section focus on how the organization shall periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	
System and Services Acquisition (SA)	The standards listed in this section focus on how the organization shall: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.	
System and Communications Protection (SC)	The standards listed in this section focus on how the organization shall: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	
System and Information Integrity (SI)	The standards listed in this section focus on how the organization shall: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories, and take appropriate actions in response.	

CMS continues to focus on protecting the health information received from its beneficiaries while processing claims. Ensuring the Confidentiality, Integrity, and Availability (CIA) of CMS sensitive information remains of paramount concern in the continuing effort to improve the overall security program. CMS continually reviews evolving Federal security standards and directives to ensure that the CMS CSRs are current and compliant with all Federal mandates. CMS provides technical clarifications to all organizations and assesses potential impacts of any updated or new requirements. The following rationales are used in preparing these modifications:

- Where Federal improvements are already covered by an existing CSR, these documents are added as references.
- Where Federal improvements are partially covered by an existing CSR, the existing CSR is modified to incorporate appropriate language and the appropriate document(s) are listed as reference(s).
- Where Federal improvements are not covered by an existing CSR, a new CSR is added and the appropriate document(s) are listed as a reference(s).

2.2.1 Security Categorization and Impact Level (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, is the mandatory Federal security categorization standard. It requires organizations to categorize their information systems based on the sensitivity of the information resident on those systems, and the impact on individual operations and assets in the event of a compromise of CIA. The standard is based on the simple and wellestablished concept of determining information system priorities, and applying reasonable and achievable measures to adequately protect those systems and the data they contain.

FIPS 199 establishes a categorization scheme for information systems as Low-impact, Moderate-impact, or High-impact for the CIA security objectives. The CMS System Security Level is based on the highest value (i.e., high water mark) determined by the CIA for each type of information resident on that information systems. The resultant high water mark is the CMS System Security Level which becomes the basis for selecting appropriate security controls and techniques for protecting CMS operations, assets, and data.

Each security control family contains the applicable security standards with the minimum security controls by security impact level, or in the case of Personnel Security (PS), the position sensitivity level (i.e., High, Moderate, or Low). These standards are designed to assist the Business Owner and system developer/maintainer in defining the information security requirements for their system.

Even though a system may need to be covered by a specific control, the Business Owner may not have to implement that control as long as he/she can demonstrate that the control is satisfied by a higher-level control. The Business Owner assisted by the system developer/maintainer is responsible for evaluating all information security areas within the CSRs and determining the appropriateness for their system.

When a control cannot be implemented even at the minimum level due to resource issues such as funding and personnel constraints or hardware/software limitations, alternative or compensating safeguards can be implemented to reduce the risk to CMS, and CMS information, information systems, and assets. This shall be considered as part of risk management and the alternative or compensating controls shall be documented in the Information Security (IS) Risk Assessment (RA) and System Security Plan (SSP), and approved by the CMS Chief Information Officer (CIO) or his/her designated representative.

2.2.2 Baseline and Enhancement Security Controls (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

To assist in making the appropriate selection of security controls for information systems, the concept of baseline controls is used. Baseline controls are the minimum security controls recommended for an information system based on the system's security categorization as defined by CMS using FIPS Pub 199. The CMS-tailored baseline security controls (i.e., CMS PISP policy statements) serve as the starting point for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems.

In many cases, enhancement controls are necessary to address specific threats to, and vulnerabilities in, an information system or to satisfy the requirements of applicable laws, *Executive Orders, directives, policies, standards, or regulations (e.g., FISMA, HIPAA, IRS, HSPD-7, OMB Circular A-130, Appendix III). Enhancement controls: (i) build in additional, but related, functionality to a baseline control; and/or (ii) increase the strength of a baseline control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment.*

Control enhancements are used in supplementing the tailored baselines to achieve the needed level of protection in accordance with a CMS assessment of risk. Moreover, baseline and enhancement controls contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate. Selecting the appropriate set of security controls to meet the specific, and sometimes unique, CMS security requirements is an important task—a task that demonstrates an organization's commitment to security and the due diligence exercised in protecting the CIA of their information and information systems.

The CSR security controls that apply depend upon the mission criticality of the system and its processing environment (e.g., a database on an Internet site as opposed to one on a non-public access mainframe, a General Support System [GSS] vs. a Major Application [MA] system). Another consideration is whether or not the system is covered by higherlevel controls, (e.g., an MA that inherits the controls from the GSS on which it operates, or a GSS or MA that inherits the controls of the CMS [or other organization] Master Security Plan). Three sets of baseline and enhancement controls are included in the CMS CSRs corresponding to the Low-impact, Moderate-impact, and High-impact levels defined in the security categorization process in FIPS 199. Each of the three control sets provide the security controls, including enhancement controls, for a particular impact level associated with a security category.

2.3 CSR *Security Control* Elements

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS CSR security controls are organized into 17 security control families (refer to Table A-1) and each CSR consists of the following elements:

- CSR Report Assessment Impact Level (i.e., High, Moderate, Low) Identifier
- Security Control Family, Identifier, and Class
- Baseline/Enhancement Control Number, Name, and Impact Level
- Baseline/Enhancement Control
- Guidance
- Applicability
- References
- Related Controls
- Assessment Procedure
 - Assessment Objective
 - o Assessment Methods and Objects

All information included in the CSR security control elements is available in the CISS during the FISMA Evaluation process and may be printed from the CISS Reports menu. Table A-2 illustrates a representative layout of the CSR security control elements which are explained in the following sections.

CMS Core Security Requirements for High Impact Level Assessments (i.e., CSR Attachment and Assessment Impact Level Identifier)				
	<i>Audit and Accountability (AU) – Technical</i> (i.e., Security Control Family and Identifier – Security Control Class)			
	AU-6 – Audit Monitoring, Analysis, and Reporting (High) (i.e., Baseline [or Enhancement] Control Number – Control Name and Impact Level)			
Control (i.e., Baseline [or Enhancement] Control Text)				
Guidance (i.e., Supplemental Guidance Text)				
Applicability: (i.e., Applicability Matrix)	References: (i.e., Source Documents)	Related Controls: (i.e.: Related CSRs)		
Assessment Procedure: AU-6.1 (i.e., Assessment Procedure section)				
Assessment Objective (i.e., Assessment Objectives)				
Assessment Methods and Objects (i.e., Assessment Methods and Objects)				

Table A-2. CSR Security Control Element Layout

2.3.1 CSR Attachments and Assessment Impact Levels (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Since CSRs are selected for FISMA Evaluations based upon a system or application CMS security categorization, CSRs are presented by security impact level (High, Moderate, or Low). So, a Moderate impact level assessment contains only the CSRs that apply to Moderate level impact assessments. To accommodate these CSR level differences, there are three (3) attachments to Appendix A:

- Attachment 1 CMS CSRs for High Impact Level Assessments
- Attachment 2 CMS CSRs for Moderate Impact Level Assessments
- Attachment 3 CMS CSRs for Low Impact Level Assessments

Although all three (3) impact levels are stored in the CISS tool, once an assessment impact level is selected, only the selected impact level CSRs are displayed during the FISMA Evaluation process. Likewise, the CISS tool normally prints only the selected impact level CSRs but a capability exists to print other impact level CSRs if desired.

2.3.2 Security Control Family, Identifier, and Class (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS has established three (3) security control classes of information security controls: Management, Operational, and Technical. This structure is consistent with the guidance established by NIST SP 800-53 (as amended).

Management security controls involve those safeguards and countermeasures that manage the security of the information and information systems, and the associated risk to CMS' assets and operations. There are four (4) control families (along with their twocharacter identifier) within the Management class that address:

- 1. Certification, Accreditation, and Security Assessments (CA)
- 2. Planning (PL)
- 3. Risk Assessment (RA)
- 4. System and Services Acquisition (SA)

Operational security controls support the day-to-day procedures and mechanisms to protect CMS' information and information systems. There are nine (9) control families (along with their two-character identifier) within the Operational class that address:

- 1. Awareness and Training (AT)
- 2. Configuration Management (CM)
- 3. Contingency Planning (CP)
- 4. Incident Response (IR)
- 5. Maintenance (MA)
- 6. Media Protection (MP)
- 7. Physical and Environmental Protection (PE)
- 8. Personnel Security (PS)
- 9. System and Information Integrity (SI)

Technical security controls are those security mechanisms employed within an information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. They are used to authorize or restrict the activities of all levels of users within an individual system by employing access based on a least-privileged and need-to-know approach. There are four (4) control families (along with their two-character identifier) within the Technical class that address:

- 1. Access Control (AC)
- 2. Audit and Accountability (AU)
- 3. Identification and Authentication (IA)
- 4. System and Communications Protection (SC)

Security control families are assigned to their respective security classes based on the dominant characteristics of the controls in that family. Many security controls have

elements logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning (CP) family is listed as an operational control but also has characteristics that are consistent with security management as well.

2.3.3 Baseline and Enhancement Control Number and Name (*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

To uniquely identify each baseline control within a security control family (e.g., Audit and Accountability), a one-up sequential number is appended to the family identifier (e.g., AU-1) to indicate the number of the control within the family. For example, AU-6 is the sixth control in the Audit and Accountability family. Additionally, a control name is assigned to the control identifier to identify each security control (e.g., AU-6 – Audit Monitoring, Analysis, and Reporting) within each control family.

To uniquely identify each enhancement control within a security control (e.g., AU-6 – Audit Monitoring, Analysis, and Reporting), a one-up sequential number is appended in parentheses to the control number to indicate the enhancement number within each control. For example, AU-6(1) is the first enhancement control in the AU-6 security control; AU-6(2) is the second, etc.

When the underlying CMS PISP policy statement requires amplification to specify CMSdefined parameters (i.e., assignment and/or selection operations), a "0" in parentheses is appended to the control number [e.g., AC-2(0), AC-7(0)] to indicate a control with CMSdefined control parameters.

While most CMS-tailored enhancement controls map directly to the controls defined in NIST SP 800-53 (as amended), there are some enhancement controls that are unique to CMS and its information systems and/or environment. These CMS-specific tailored controls are included as enhancements within NIST SP 800-53 security control baselines. These enhancements are included within an appropriate security control family (e.g., AC) and security control (e.g., AC-2), and identified using the baseline control number followed by the characters "CMS-" and a sequential number in parenthesis. For example, AC-2(CMS-1) designates the first CMS-specific enhancement to security control AC-2, and AC-2(CMS-2) designates the second.

There are several instances where a CMS-specific enhancement control does not map to an existing baseline control defined in NIST SP 800-53 (as amended). In those cases, a new baseline security control was created within an appropriate existing security control family. These new CMS-specific baseline control include the two-character security family identifier followed by the characters "CMS-" and a one-up sequential number. For example, SC-CMS-1 designates the first new CMS-specific baseline control in the SC security family and SC-CMS-3 designates the third. All enhancement controls to these new CMS-specific baseline controls are then designated using the numbering sequences explained in the previous paragraphs [e.g., SC-CMS-3(CMS-0), SC-CMS-3(CMS-1)]. In addition to CMS-tailored enhancement controls, there are additional security controls that apply to CMS and/or its organizations based on the type of information being stored, accessed, processed, and/or transmitted on their information systems. These enhancements are required by Federal laws, Executive Orders, or directives (e.g., IRS, FISCAM, HSPD-7, HIPAA, CMS-directed requirements).

Some of these additional security controls are already included in existing CMS CSRs, so they do not require separate or additional CSR controls. The security controls that are not already covered by existing CSRs are included as CISS-selectable enhancement controls. For example, FISCAM enhancement controls can be selected (i.e., added) to the CMS minimum baseline controls when required to meet those additional security control requirements. This type of enhancement control includes the standard baseline security control number followed by a unique three-letter character identifier and a one-up sequential number in parentheses. The following three-letter characters identify these additional enhancement controls within the CMS CSRs:

- DIR Directed by CMS (includes controls not currently included in the CMS ARS but required by CMS [e.g., PE-3(DIR-1)]
- FIS FISCAM-unique controls [e.g., AC-2(FIS-1)]
- *IRS IRS Pub 1075-unique controls required to protect identifiable Federal Taxpayer Information (FTI) [e.g., MP-6(IRS-1)]*
- *PII Personally Identifiable Information including HIPAA Electronic Protected Health Information [EPHI] this is not unique to HIPAA and/or IRS information that is not identifiable FTI [e.g., AC-20(PII-1)]*

2.3.4 Control

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Control section provides a concise statement of the specific security control capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be performed by the organization or by the information system.

The baseline and enhancement security controls shall be viewed as the foundation or starting point in the selection of adequate security controls for an information system. The security controls represent, for a particular class of information system, the starting point for demonstrating the needed level of security due diligence by an organization in the protection of its operations and assets.

In many cases, enhancement controls are used to supplement baseline controls. Enhancement controls are numbered sequentially within each control so the enhancements can be easily identified when selected to supplement the basic control. The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements. (Refer to section 2.3.2 above for control numbering.)

The CISS CSRs provide the minimum security controls for information systems, arranged by control families, and selectable by impact level. The CSRs represent the entire set of minimum security controls as defined by CMS at this time.

All CSR baseline security controls are applicable to all organizations unless specifically identified as "Not required" in the CMS CSRs within a specific security level. When a baseline control is "Not required" in the with a specific security level, there will not be any enhancement controls stated for that control identifier.

2.3.5 *Guidance* (*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

The Guidance section provides supplemental information related to a specific security control when deemed necessary or appropriate. Organizations are expected to apply the guidance as appropriate, when defining, developing, and implementing security controls. In certain instances, the guidance provides more detail concerning the control requirements or important considerations (and the needed flexibility) for implementing security controls in the context of an organization's operational environment, specific mission requirements, or assessment of risk. In addition, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST SPs) are listed in the guidance section, when appropriate, for the particular security control.

2.3.6 Applicability

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All CSRs in a selected control set apply UNLESS a specific contract/entity type is specified as an exception in the Applicability section. Because CMS may add new contract types and/or systems that use the CISS for their FISMA Evaluation, due diligence requires that all security controls be met unless a control is deemed optional for a specific contract/entity type. Refer to the legend below for the current CMS contract types.

Applicability Exception Legend: ABMAC – A/B Medicare Administrative Contractor COB – Coordination of Benefits CWF – Common Working File [Host] DC – Data Center DMEMAC – Durable Medical Equipment Medicare Administrative Contractor EDC – Enterprise Data Center PartA – Part A Fiscal Intermediary PartB – Part B Carrier PSC – Program Safeguard Contractor QIC – Quality Integrity Contractor RAC – Recovery Audit Contractor SS – Standard System [Maintainer] ZPIC – Zone Program Integrity Contractor

Refer to section 2.4.1 for a brief discussion of the FISMA Evaluation control selection process to the CISS User Guide for instructions on selecting FISMA Evaluation controls.

2.3.7 References (*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

The References section identifies the source documents and section or paragraph designations that are the basis or source for the applicable CSR security control. Because the CSRs retain their source references, organizations can conduct "modular" FISMA Evaluations that address the likely audit procedures that would be used by an external audit agency. For example, to prepare for a FISCAM-related audit, an organization's ISSO/SSO might review all the CSRs specifically associated with the FISCAM. In addition, the ISSO/SSO could use references in the CISS database to determine the location of a specific FISCAM requirement.

2.3.8 Related Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Many, but not all, CSRs may be related to one or more other CSR security control. When addressing some CSRs, it may be important that their responses be consistent with one or more related CSRs. At the very least, organizations shall take care to ensure that related CSR responses do not conflict. While every effort was made to identify related CSRs, other unidentified relationships may exist that are unique to a particular system, contract type, or organization.

2.3.9 Assessment Procedures (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Assessment Procedures section (i.e., Assessment Objectives, and Assessment Methods and Objects) in the CSRs directly support the validation of individual control effectiveness. The primary objective of the Assessment Procedures is to help determine if the security controls in the information system are effective in their application (i.e., implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system). The security Assessment Procedures defined in the CSRs provide a foundational level of assessment to support the security certification process. The Assessment Procedures are identified using their applicable control identifier (e.g., AC-1, AC-2(1), etc.) followed by a numerical decimal identifier (e.g., AC-1.1, AC-2(1).1, etc.)

2.3.9.1 Assessment Objective

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Assessment Procedure consists of a set of procedural steps that are designed to achieve one or more assessment objectives by applying assessment methods to assessment objects.

The Assessment Objectives include a set of determination statements ("Determine if...") related to the particular security control under assessment. The determination statements are closely linked to the content of the security control (i.e., the security control functionality) to ensure traceability of assessment results back to the fundamental control requirements.

Assessment Objectives establish the expectations for security control assessments based on the assurance requirements defined in the security control. The assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness. Each of the Assessment Objective determination statements is either traceable to requirements in the baseline or enhancement security control, or the guidance. This ensures that all aspects of the security control are assessed and that any weaknesses or deficiencies in the control can be identified and remediation actions taken.

NIST SP 800-53A (as amended), Appendix E, Assessment Expectations, provides an explanation of the expectations of security assessments by impact level. These assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness. Organizations are expected to review and use the NIST SP 800-53A assessment expectations as guidance during their FISMA Evaluations.

Table A-3 summarizes the assessment expectations for Low-impact, Moderate-impact, and High-impact information systems.

Assessment Expectations	Information System Impact Level		
	Low	Moderate	High
Security controls are in place with no obvious errors.	\checkmark	\checkmark	\checkmark
Increased grounds for confidence that the security controls are implemented correctly and operating as intended.	_	\checkmark	\checkmark
Further increased grounds for confidence that the security controls are implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	_	_	V

Table A-3. Assessment Expectations by Information System Impact Level

The decision to reduce the level of effort for the assessment of security controls in Lowimpact and Moderate-impact information systems does not affect the basic requirements in the control as stated in the CMS CSRs. The decision to employ optional determination statements and assessment methods shall be a decision guided by an organizational assessment of risk with input from key organizational officials with a vested interest in the assessment and with responsibility for carrying out or supporting CMS missions and business functions.

2.3.9.2 Assessment Methods and Objects (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Assessment Procedure consists of a set of procedural steps that are created to achieve one or more Assessment Objectives by applying assessment methods to assessment objects. As stated in the previous section, the assessment objectives include a set of determination statements related to the particular security control under assessment. The application of assessment procedures to a security control produces assessment findings. These assessment findings are subsequently used in helping to determine the overall effectiveness of the security control.

The three (3) assessment methods defined in the processing component of the framework include Examine, Interview, and Test. NIST SP 800-53A (as amended), Appendix D, Assessment Method Descriptions, provides a detailed explanation of these three (3) assessment methods. Organizations are expected to review and use the NIST SP 800-53A assessment method explanations as guidance during their FISMA Evaluations.

Table A-4 summarizes the hierarchal order of the three (3) assessment methods and their definition.

Assessment Method	Definition
Examine	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities) to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.
Interview	The process of conducting focused discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.
Test	The process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of the security control effectiveness.

Table A-4. Assessment Method Hierarchy and Definitions

Each of the assessment methods (Examine, Interview, and Test) includes a set of attributes: Depth and Coverage. NIST SP 800-53A (as amended), Appendix D, Assessment Method Descriptions, provides detailed explanations of the assessment method Depth and Coverage attribute values. Organizations are expected to review and use the NIST SP 800-53A assessment method depth and coverage attribute value explanations as guidance during their FISMA Evaluations.

Table A-5 summarizes the assessment method attributes values by information system impact level.

Assessment Methods Examine, Interview, Test	Information System Impact Level		
Attribute		Moderate	High
Depth	Generalized	Focused	Detailed
Coverage	Representative	Specific	Comprehensive

 Table A-5. Assessment Method Attributes and Attribute Values by Impact Level

The attribute values for the assessment methods (which describe the rigor and level of detail associated with the assessment) are hierarchical in nature. For the Depth attribute, the Focused attribute value includes and builds upon the assessment rigor and level of detail defined for the Generalized attribute value; the Detailed attribute value includes and builds upon the assessment rigor and level of detail defined for the Generalized attribute value; the Detailed attribute value includes and builds upon the assessment rigor and level of detail defined for the Focused attribute, the Specific attribute value includes and builds upon the number and type of assessment objects defined for the Representative attribute value; the Comprehensive attribute value includes and builds upon the number and type of assessment objects and builds upon the number and type of assessment objects defined for the number and type of assessment objects defined for the number and type of assessment objects defined for the number and type of assessment objects defined for the number and type of assessment objects defined for the number and type of assessment objects defined for the number and type of assessment objects defined for the number and type of assessment objects defined for the Networks.

NIST SP 800-53A (as amended), Appendix E, Assessment Expectations, provides detailed explanations of the assessment objects. Organizations are expected to review and use the NIST SP 800-53A assessment object explanations as guidance during their FISMA Evaluations.

Table A-6 summarizes the assessment objects and their definitions.

Assessment Object	Definition
Specifications	The document-based artifacts (e.g., policies, plans, procedures, system requirements, designs) associated with an information system.
Mechanisms	The specific hardware, software, or firmware safeguards and countermeasures employed within an information system. These also include physical protection devices associated with an information system (e.g., locks, keypads, security cameras, fire protection devices, fireproof safes).
Activities	The specific protection-related pursuits or actions supporting an information system that involve people (e.g., system operations, administration, and management; exercises).
Individuals	The people or groups of people applying the specifications, mechanisms, or activities described above.

Table A-6. Assessment Objects and Definitions

Recognizing that organizations can specify, organize, document, and configure their information systems in a variety of ways, the assessment objects identified in the CSRs that are provided in conjunction with the Interview, Examine, and Test assessment methods shall be considered suggested objects where information/evidence may be found. As such, assessors are expected to use their judgment in applying the designated assessment methods to the associated set of assessment objects. Each assessment method listed in a procedural step shall be applied to a sufficient number of assessment objects to produce the information necessary to make the determination in the determination statement and to satisfy the assessment objective. It may not always be necessary (or possible) to apply each assessment method to every assessment object in the CSR list.

2.4 Completing the *FISMA Evaluation*

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A critical factor for maintaining on-going compliance with FISMA and the Federal Managers' Financial Integrity Act (FMFIA) of 1982, is for Business Owners in coordination with developers, maintainers, and system operators, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing) and person hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of corrective action plans (CAP) for vulnerabilities noted during the testing.

The purpose of annual FISMA Evaluation is to examine and analyze implemented security safeguards in order to provide evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. The annual FISMA Evaluation is intended to test the security controls to determine the extent to which the controls are:

- *implemented correctly,*
- operating as intended, and
- producing the desired outcome with respect to meeting the security requirements for the system.

The CISS *FISMA Evaluation module* is where *organizations* indicate their compliance with each CSR. *Organizations* select a Status, and provide a descriptive text response that provides details of the Status marked for that CSR.

2.4.1 FISMA Evaluation Control Selection (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The annual FISMA testing requirement has been interpreted by the OMB as being within 365 calendar days of the prior test. Over a three (3) year period, all controls applicable to a system or application shall be tested. This means a subset (no less than one-third $[^{1}/_{3}]$) of the security controls shall be tested each year so that all controls are tested during a three (3) year period. This annual subset is inclusive of the required annual test of the system or application Contingency Plan.

While CMS does not mandate which subset of controls shall be tested each year or require a specific number of controls to be tested each year, CMS (and OMB) does require that all controls be tested within a three (3) year period. Business Owners, in coordination with the developer/maintainers of CMS applications and systems, are responsible for meeting this requirement.

The FISMA Evaluation control selection is performed by CISS based on several factors determined through user interview questions/responses. The primary selection factor is the system or application impact level (i.e., High, Moderate, Low). Other selection factors include the type of information handled by the system or application (e.g., PII, FTI) or the source references that apply to the system or application (e.g., FISCAM, IRS). Refer to the CISS User Guide for instructions on selecting FISMA Evaluation controls.

2.4.2 Security Control Assessment (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Security assessments (e.g., FISMA Evaluations) are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits. Rather, they are the last line of defense in the process of identifying the strengths and weaknesses of the organization's information system that supports critical Federal applications and missions in a global environment of sophisticated threats. The findings produced by security assessors during the FISMA Evaluation are used primarily to determine the overall effectiveness of the security controls in an information system, and to provide credible and meaningful inputs to the organization's security accreditation process. A well-executed security assessment helps to determine the validity of the security controls identified in the information SSP and to facilitate a cost-effective approach to correcting any deficiencies in the system in an orderly and disciplined manner consistent with the organization's mission requirements.

FISMA Evaluations using the assessment procedures (i.e., Assessment Objectives, and Assessment Methods and Objects) provided with each CSR are not intended to make judgments on the necessity or sufficiency of the set of security controls documented in the SSP. Rather the assessment procedures are applied to determine if the security controls employed (and required under CMS policy) within the information system are, in fact, implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Assessors, in the course of executing the procedures within the CSRs, might discover potential errors or oversights in the security plan and shall determine how those potential errors or oversights may affect the CIA of the information system in the event of a compromise or breach of the system. Such discoveries and determinations, however, are a by-product of the assessment and not the purpose of the assessment. Therefore, while assessors are expected to notify appropriate organizational officials about any potential problems with the SSP, assessors are not empowered to second-guess or question the decisions of mission/system owners and authorizing officials concerning the impact level of the information system or the security control selection and supplementation activities, which include the tailoring and supplementation of the security control baselines in the CMS CSRs.

Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling/producing the information necessary to make the determination associated with each assessment objective. Each determination statement in a procedural step contained within an assessment procedure executed by an assessor produces one the following results: (i) Met; or (ii) Not Met. These assessment results are described in Table A-7.

Level	Description
Met	Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result.
Not Met	Indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates potential anomalies in the operation or implementation of the control that may need to be addressed by the organization.

Table A-7. Assessment Results

A result of "Not Met" may also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient evidence to make the particular determination called for in the determination statement. The assessor results (i.e., the determinations made) shall be an objective reporting of what was found concerning the security control assessed. For each assessment result of other than "Met," assessors shall indicate which parts of the security control are affected by the finding (i.e., those aspects of the control that were deemed not met or were not able to be assessed) and describe how the control differs from the planned or expected state. Any potential for compromises to confidentiality, integrity, and availability due to a "Not Met" finding shall also be noted by the assessor.

The assessor results are aggregated and documented for each control requirement in the CISS FISMA Evaluation (refer to the CISS User Guide) and they serve as a primary information source for the POA&M. The assessor does not prepare the POA&M, but may provide recommendations for its content. The Business Owner may have an opportunity to address some or all of the weaknesses or deficiencies in the security controls identified during the assessment before those weaknesses or deficiencies become part of the POA&M. However, senior leadership involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in some priority order—first providing resources to the information systems that are supporting the most critical and sensitive missions for the organization. Each identified Finding and corresponding Weakness shall be addressed with a corrective Action Plan in the CISS before submission of the FISMA Evaluation to CMS.

Ultimately, the assessment results and any subsequent mitigation actions initiated by the Business Owner in collaboration with designated organizational officials trigger updates to the IS RA and the SSP. Therefore, the key documents used by the authorizing official to determine the security status of the information system (i.e., SSP with updated IS RA, security assessment report, and POA&M) are updated to reflect the results of the security assessment.

2.5 All *CSR* Responses

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The following information and guidance *shall* be considered when evaluating all CSRs and preparing *FISMA Evaluation* CSR responses *in the CISS*:

- a) Each CSR *response* requires a *compliance* Status (i.e., *Met*, *Not Met*, *or Not Applicable* [*N*/*A*]) to be selected, *accompanied by* a detailed explanation in the Response Comment/Explanation field *that provides* a complete description of What, Where, Why, and How each CSR *element* is or is not *met*.
- b) A reference to the applicable section, page, or paragraph of the FISMA Evaluation working papers where the applicable Assessment Procedure was performed and documented. (A single copy of the FISMA Evaluation working papers shall be attached electronically the FISMA Evaluation Audit/Review record in the CISS Tool.)

- c) Every CSR response requires that a principle Point-of-Contact (POC) be designated. The CISS provides a specific field for this information, and the field requires that at least one POC value be entered. Other interested POCs may also be assigned to a CSR as non-primary designees. However, one and only one primary POC *shall* be assigned to each CSR response.
- d) Organizations should be aware that even if data processing duties are subcontracted out to either another CMS organization (such as a data center) or to a third-party subcontractor (such as a business services company), responsibility for the implementation and evaluation of security controls ultimately resides with the primary contract holder. Organizations shall coordinate the establishment of boundaries for specific issues. While this does not necessarily require a sharing of FISMA Evaluation responses, it does require that organizations communicate and coordinate among themselves such that interfaces of responsibilities for particular CSRs are addressed by all responsible organizations without gaps in coverage.
- e) Where a merging of responsibilities occurs among *organizations* (such as the interface between data centers, claims processors, and standard system maintainers), a detailed description of these interfaces and the division of responsibilities *shall* be provided in the Response Comment/Explanation field. The description *shall* include local responsibilities as well as those that are perceived to be responsibilities of some other CMS *organization*.
- f) Each CSR in the CISS includes an Applicability section, which identifies those CMS contract/entity types (i.e., Part A, Part B, CWF, etc.) where specific CSRs may not apply. The purpose of the Applicability section is not to summarily exclude CSRs from a particular contract/entity type. The Applicability section is designed to be used as a guide. CMS recognizes that system configurations vary widely throughout the CMS community; therefore, each organization shall evaluate and report on each CSR's applicability to its own systems.
- g) *Organizations* should also be aware of the CSR terms included in the BPSSM Glossary (Appendix H) and address the CSRs as they apply to their local environment. For example, the term "data center" *(i.e., computer facility) is defined as* "a site or location *with computer hardware* where information processing is performed" (e.g., claims entry and processing). This term is not limited to any specific CMS Enterprise Data Center (EDC) or Carrier/F1 Data Center environment. A "system" may include mainframe systems, desktop systems, workstations and servers, networks, and any platform regardless of the operating system. "System software" includes the operating system and utility programs (e.g., workstation, server, and network software and utilities) and is distinguished from application software. "Application software" includes the standard system (i.e., *MA*) but it also includes any computer program (i.e., application) that manipulates data or performs a specific function (e.g., front-end and back-end applications).

h) If *organizational* policy conflicts with a CMS CSR, a detailed explanation *shall* be provided as to why the *organization* policy cannot be modified to apply to CMS data. Any conflicts with *organization* policy (in which the final disposition of the CSR response would not ultimately result in full compliance with CMS requirements) *shall* be addressed for resolution, by written correspondence with the CMS Central Office, prior to indicating *such a non-compliance status* in any CSR response.

Organizations are required to enter a current *compliance* status (*Met, Not Met, N/A*) and a detailed Comment/Explanation for each CSR. The annual *FISMA Evaluation* is one of the central *security* documents in *an organization*'s security profile and *shall* reflect sufficient detail to convey to CMS the current status of the *organization*'s security program.

2.6 "Not Applicable" (N/A) Response Status (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A response status of "N/A" indicates that the *CSR security control* requirements *may* not *be* applicable to the *organization*. CMS expects most, if not all, CSRs to apply to all portions of all *CMS* contracts *and expects all CSRs to be evaluated as to their* applicability. Very few CSRs are expected to receive "N/A" responses. The Response Comment/Explanation field *shall* contain a detailed explanation of the circumstances that render this CSR non-applicable (regardless of whether this CSR is listed as *not* applicable in *A*pplicability matrix for a particular contract type), and how this information can be verified, in a format that clearly answers each question described below:

a) Why is this CSR not applicable?

A complete and detailed description *shall* be provided to describe the circumstances that render the subject CSR "N/A" to a particular *organization*. Referral to the Applicability matrix is NOT sufficient justification for an "N/A" response. A full understanding of the reasons for non-applicability *shall* be demonstrated and explained in the CSR response. This is *necessary* because the Applicability matrix is not definitive, and CMS anticipates cases in which a CSR will indeed apply to one or more *organizations* even when the CISS Applicability matrix indicates it generally does not. CMS approvals (and the citation[s] thereof) are not required for "N/A" responses that are corroborated by the CISS Applicability *matrix*.

- b) How did you verify this status with CMS?
 - i. **Applicability matrix** *indicates* **CSR** is **NOT applicable.** CMS approvals (and the citation[s] thereof) are not required for "N/A" responses that are corroborated by the CISS Applicability matrix. *However, an explanation is required amplifying why the organization agrees that the CSR is "N/A."*

- ii. **Applicability matrix** *indicates* **CSR is applicable.** In the case of an "N/A" response that is not corroborated by the Applicability matrix, CMS approval *shall* be obtained and documented, and such documentation *shall* be provided with the CSR response (see below). Note that CMS approval must be renewed each year for each "N/A" CSR *that is not corroborated by the Applicability matrix*.
- iii. Conditional CSR. A conditional CSR is a control prefixed with a conditional "If" statement (e.g., "If automated information labeling is utilized..." or "If wireless access is explicitly approved..."). For conditional CSRs where the conditional control is not required to be used or implemented (i.e., automated information labeling is not used), a "Met" response, with an explanation detailing that the required preconditions do not exist, is appropriate.

The CISS requires that copies of the associated CMS approval documentation *be* **attached to the CSR response within the CISS tool.** Approvals for prior years may be cited in requests for CMS approval for the current year response but *prior year approvals* cannot be used as documentation of CMS approval for the current year CSR "N/A" response. Each year, the CMS approval process *shall* be repeated (unless specifically stated *otherwise* in the CMS-provided approval documentation).

In addition to the requirements stated above in section 2.6.a), include the following information with *each* CMS-approved "N/A" response:

- (1) Date CMS approved the response,
- (2) CMS office that approved the response, and
- (3) Attached documentation of CMS concurrence (e-mail text file, or letter/document).

2.7 *Compliance Status* (*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

Testing of the CSR compliance will result in one of two FISMA compliance control status: "Met" or "Not Met." Other than the "N/A" response (which indicates that the control requirement is not required) explained in Section 2.6, "Met" and "Not Met" are the only CSR status responses available in the CISS to report a FISMA Evaluation result. To determine compliance, the CSR Assessment Procedures provided with each CSR shall be applied to determine if the security controls as employed within the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the applicable security requirement. As stated previously, baseline controls are the minimum security controls recommended for an information system based on the system's security categorization. Enhancement controls provide additional, but related, functionality to a baseline control; and increase the strength of the baseline control. Although each baseline and enhancement control is assessed separately and its compliance status is recorded separately, the CISS does not allow a baseline control group (e.g., AC-1, AC-2, AC-3, etc.) to be fully compliant unless all of the control group enhancements are also compliant [e.g., AC-2(1), AC-2(2), AC-2(3), etc.]. The CISS automatically determines overall control group compliance and provides feedback when a control group is not compliant (refer to the CISS User Guide for additional information).

The decision tree in Figure A-1 has been developed to help organizations establish their CSR compliance status for each baseline and enhancement control.

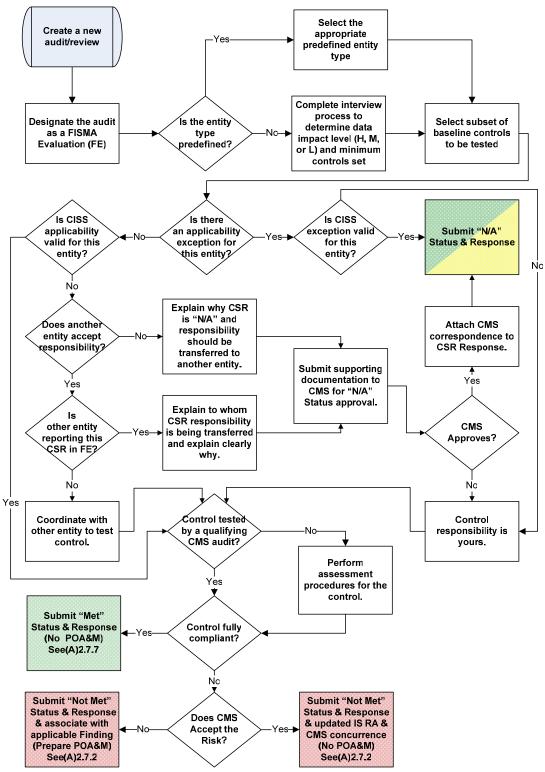


Figure A-1. Response Status Decision Tree

2.7.1 *"Met"* Response Status

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Response Comment/Explanation field *shall*, at a minimum, contain a detailed explanation of how the stipulations of the CSR are being met, and how compliance can be verified, in a format that clearly answers each question described below:

a) Who performed the evaluation?

Each CSR response shall include a reference to the applicable Audit/Review in which the applicable CSR was tested. From this reference, the entity that performed the Evaluation of the applicable control may be determined. Within the CISS, the default Audit/Review will be the current FISMA Evaluation. However, other qualifying Audit/Reviews may be referenced (such as a qualifying SAS 70, or other audit.) If another qualifying management-directed audit/review performed the applicable CSR Assessment Procedures (or their equivalent), those results may be used as support for the current FISMA Evaluation. In this case, the Assessment Procedures do not need to be repeated.

All management-directed and independent testing conducted within 365 days of the attestation due date may be used to meet the requirement for annual security controls testing. Management-directed and independent testing includes:

- *Certification and Accreditation (C&A) independent ST&E testing,*
- OMB Circular A-123 IT EDP assessment,
- Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) Section 912 evaluations,
- MMA Testing,
- Statement on Auditing Standard (SAS) 70 reviews,
- Certification Package for Internal Controls (CPIC) audits,
- General Accounting Office (GAO) reviews,
- FE testing, and
- Testing results from local test teams (i.e., organizationally separated from the Medicare operations team) organized for purposes of meeting this requirement.

Testing pursuant to the Chief Financial Officer (CFO) audit of CMS financial statements cannot be used. CFO testing is directed by the Office of the Inspector General (OIG) and is not considered management-directed.

b) What can be used to verify full compliance?

While not required to be included as supporting documentation in the FISMA Evaluation submission, documentation in the form of policies, procedures, manuals, employee training records, and logs shall be available to verify compliance. A description of these documents shall be included in the

Comment/Explanation field. The control shall be tested using the CSR Assessment Procedures (i.e., Assessment Objective, and Assessment Methods and Objects) to verify compliance. All documentation specified in the CSR shall be verified for a response to be considered complete.

c) Where can the applicable *evaluation* documentation be found?

Verification of the performance of the applicable Assessment procedures for each CSR is a fundamental part of the FISMA Evaluation process. Methods of verification in accordance with the applicable CSR Assessment Procedures should be accessible to reviewers. Ensure that a cross reference to section/page/paragraph in the working papers of the applicable audit/review documentation is clearly described. The applicable referenced working papers shall also be provided with the overall FISMA Evaluation. If another audit or review is cited as the source of testing, applicable working papers for the referenced audit/review shall also be included (electronically) with the FISMA Evaluation.

- d) How exactly *are* the CSR *assessment objectives being* met?
 - i. Do not include planned controls or controls that are not fully implemented. If all components are not fully in place, the response status *shall* be changed to *"Not Met"* and a suitable Weakness/Action Plan combination identified.
 - ii. In some cases, alternative controls might be implemented to achieve the intent of the CSR. Ensure that information about implementation of alternative controls to meet the specifics of the applicable CSR is sufficiently detailed for CMS to determine if the alternative controls are acceptable.

To be effective, *FISMA Evaluations shall* include tests and examinations of security controls. *The evaluations shall be conducted using the applicable Assessment Procedures.*

2.7.2 "Not Met" Response Status (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A response status of "Not Met" implies that the assessment information obtained during the evaluation indicates potential anomalies in the operation or implementation of the control that will need to be addressed by the organization. A status of "Not Met" may also indicate that for reasons specified in the assessment report (and entered in the CSR Response), the assessor was unable to obtain sufficient evidence to make the particular determination called for in the determination statement (i.e., Assessment Objectives). For each assessment status of "Not Met," assessors shall indicate which parts of the security control are affected by the assessment finding (i.e., those aspects of the control that were deemed not met or were not able to be assessed) and describe how the control differs from the planned or expected state, and this information shall be entered in the applicable CSR Response Comment/Explanation field.

- A "Not Met" CSR status results in one of the following:
 - a) **Finding.** The status of each CSR baseline and enhancement shall be fully compliant or "Met." For any response status that is not compliant, the [Finding] button on the CISS FISMA Evaluation form is enabled. An appropriate Finding (and associated Weakness)/Action Plan combination shall accompany any CSR response that is "Not Met."
 - b) **Risk-Based Decision.** In extremely rare cases, full compliance of a CSR minimum security requirement may present unacceptable fiscal or configuration barriers. In such cases, CMS may agree that the risk is acceptable for the present and no Finding/Action Plan combination is required or desired. In such cases, prior CMS concurrence is required AND a full assessment of all of the implications of not being in full compliance of the minimum security requirements for the applicable CSR is fully documented in the associated system IS RA. BOTH the updated IS RA AND full documentation of CMS concurrence SHALL be attached to the CSR response.

2.8 Findings and Weaknesses

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Weaknesses form the basis for CISS Action Plans (see section 2.9 of this appendix for a description of Action Plans). *Audit* Findings, *which include FISMA Evaluation* non-compliant CSR *Findings*, form the basis of Weaknesses.

Every Finding *shall* be addressed by a Weakness record in the CISS. A Finding is any deficiency identified and reported during an audit or review—whether internal or external. For example:

"Login accounts exist for employees who have left the company."

A Weakness, in this context, would be the underlying cause for, or source of, the Finding. For example:

"No policy exists for the removal of accounts when employees leave."

A FISMA Evaluation Finding can be associated with one or more non-compliant CSRs but only if the security controls or assessment findings are related. A Weakness shall be identified for each Finding; *h*owever, a single Weakness may address several Findings. Consider the following simplified illustration:

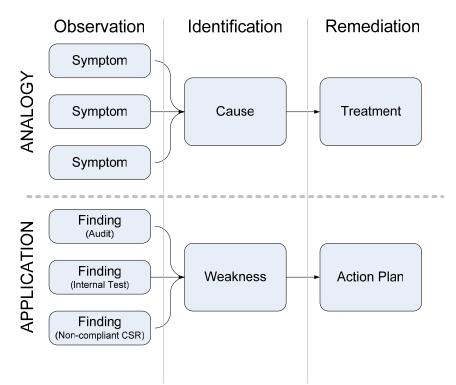


Figure A-2. Analogy for Finding-Weakness-Action Plan Relationship

An Action Plan *shall* be designated to address each Weakness.

Weaknesses that need to be recorded and tracked can be identified either reactively or proactively. Reactive Weakness determination indicates that outside auditors or reviewers identified Findings leading to the Weakness determination. Proactive Weakness determination occurs by conducting regular program and system reviews using *FISMA Evaluation*s or internal reviews. Sources of security-related Findings and Weaknesses include, but are not limited to:

- Chief Financial Officer (CFO)/Electronic Data Processing (EDP) Audits related to annual CFO Financial Statement Audits (which may include network vulnerability assessment/security testing /NVA/ST/)
- Statement on Auditing Standards No. 70 (SAS 70) Audits
- Submission of a Certification Package for Internal Controls (CPIC)
- HHS OIG IT Controls Assessment
- Financial reviews conducted by the General Accounting Office (GAO)

- Section 912 Evaluations or Testing
- Data Center System Tests
- Penetration/External Vulnerability Assessment (EVA) Tests
- FISMA Evaluations
- Information Security Risk Assessments
- Internal or <u>Self-directed Reviews</u>, <u>Audits</u>, or <u>Tests</u>

This list is not exhaustive; there are many avenues for discovering Weaknesses. In the CISS, a*ll Findings and* Weakness*es are* considered to have resulted from some type of audit or review.

The flow in Figure A-3 has been developed to assist organizations establish the linkage among Findings, Weaknesses, and Action Plans.

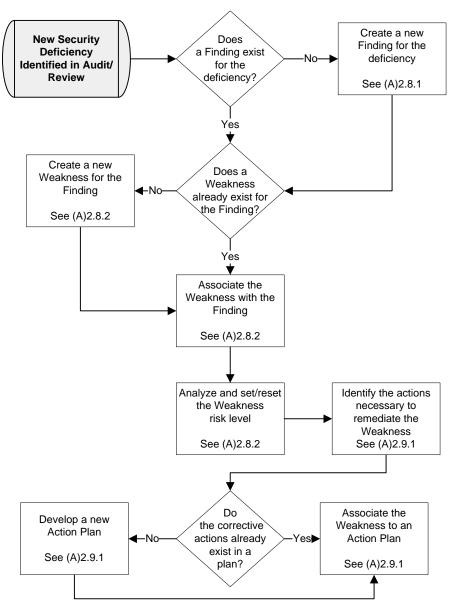


Figure A-3. Weakness Decision Tree

2.8.1 Findings

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All security-related Findings identified or reported by internal or external audits and reviews *shall* be entered into the CISS and associated with (i.e., linked to) one Weakness.

The following subsections provide guidance for populating the CISS Findings form. Consult the CISS User Guide for specific instructions related to accessing and working with CISS Findings form components.

2.8.1.1 Finding Identifier

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Finding identifier is normally the same identifier provided in the audit or review report. If an internal Finding is identified, the Finding is recorded by a unique identifier consisting of the following information:

a) **Entity.** The first three (3) to five (5) characters identify the name of the contractor. These *entity-identifiers* are listed under contractor abbreviations in Chapter 7, Internal Control Requirements, section 40.3, CMS Finding Numbers, of the Medicare Financial Manual (CMS Pub 100-6).

NOTE: This unique *entity*-identifier is not reported to agencies outside of CMS nor is it included in CMS' annual or quarterly POA&M submissions to OMB. Findings reported outside CMS cannot be traced to a *CMS organization or contractor*.

- b) **Year.** The next four (4) digits denote the Fiscal Year (FY) in which the Finding was identified and first reported. The year is normally the same as assigned in the audit or review report.
- c) **Code.** The next one (1) or two (2) characters identifies the type of review or audit. They are as follows:
 - 9E Section 912 Evaluation
 - 9T Section 912 Testing
 - A A-123 Non-IT Assessment
 - AT Authority to Operate
 - *C CPIC*, (Your annual self certification package)
 - CA Certification and Accreditation
 - CP Contingency Plan
 - DR CFO Desktop Review
 - *E CFO EDP Review*
 - *F CFO Financial Review*
 - FE FISMA Evaluation
 - G GAO Reviews (Financial Reviews)
 - I A-123 IT (EDP) Assessment
 - *IR* Internal reviews initiated by the entity to meet other Federal requirements
 - *M CMS CPIC Workgroup Reviews*
 - N SAS 70 Novation
 - *O* OIG Reviews (HHS Office of Inspector General [IT] Controls Assessment)
 - P CMS 1522 Workgroup Reviews
 - *R Accounts Receivable Review*
 - RA Risk Assessments
 - *S* Statement on Auditing Standards No. 70 (SAS 70)
 - SP System Security Plan

V CFO Related NVA/ST

d) **Num.** The next three (3) digits are the sequential Finding number assigned to each individual Finding beginning with 001, 002, 003, etc. The number is normally the same as assigned in the audit or review report.

2.8.1.2 Finding Title and Description

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Finding title *shall* not include any contractor-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the contractor reporting the Finding, or the location, facility, system, or application to which the Finding refers. Some appropriate Finding titles might include: "inadequate password controls," "insufficient or inconsistent data integrity controls," "inadequate firewall configuration reviews," "background investigations not performed prior to system access," "insufficient physical access controls," etc.

The intent is to provide a title that is descriptive but does not reveal sensitive or exploitable information, such as: "Telnet port open, allowing access by outside users." The title *shall* also be unique enough to be more readily identifiable by name than by number. The Finding title reported in the audit or review report *shall* generally be used, unless that title is too long or contains sensitive descriptive information.

The Finding description *shall* be the descriptive Finding information reported in the audit or review report. This description is not reported beyond CMS, so there is no restriction on its content. If the Finding is the result of an internal audit or review, the description *shall* include the Finding information required by the GAO, "Government Auditing Standards," GAO-03-673G (<u>http://www.gao.gov/govaud/yb2003.pdf</u>), commonly referred to as the "Yellow Book."

2.8.1.3 Finding Status

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All security-related Findings *shall* include a status that indicates the stage or state of the Finding corrective action. Since a Weakness may be associated with multiple Findings, one or more Findings associated with the Weakness can be closed while the Weakness remains open. The four *(4)* Finding status reporting choices are:

• **On-going.** The Finding remains open and action is on-going to correct it. However, if the Initial Target Completion Date entered in the Action Plan has passed and action is still on-going to correct the Weakness, the status *shall* be reported as Delayed.

- **Closed Pending.** (1) If the Finding was discovered in an internal review, the *organization may* proceed directly to the Closed status. (2) If the Finding was reported by a CMS initiated audit or review, the *organization* should use this status when it considers the Finding closed. However, CMS requires this type of Finding closure to be validated before it is considered Closed. The *organization* should continue to report the status as Closed Pending until the closure is validated and CMS provides documentation confirming the Closed status. The CISS will require that appropriate documentation be attached to this status to confirm the closure. This documentation *shall* address all aspects of the stated Finding and be sufficient for CMS validation of closure.
- **Closed.** If a Finding has been officially closed by CMS, *with supporting documentation as proof submitted* to the *organization*, it should be reported as Closed in the CISS. The CISS will require that appropriate missing or updated documentation not previously sent be attached to this Closed status to confirm the closure. This documentation *shall* also include any CMS closure letters.
- **Delayed.** Action is on-going to correct the Finding but the Initial Target Completion Date entered in the Action Plan has passed. The Finding should continue to be reported as Delayed until the Finding is corrected and reported as closed.

2.8.1.4 Determination of Finding Risk Level

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FISMA guidance requires that all Weaknesses be prioritized to ensure that significant IT security Weaknesses take precedence and are immediately mitigated. Since a Finding indicates a Weakness, a risk level *shall* also be assigned to each Finding.

System Finding risk levels should be determined in the system's risk assessment. The risk level determination process is the same for both Findings and Weaknesses and is summarized in section 2.8.2.9, Determining Risk.

2.8.1.5 Finding FMFIA and CPIC Severity

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Findings, and their associated Weaknesses, *shall* be disclosed as Material Weaknesses or Reportable Conditions if they have an impact on the contractor's internal control structure. Every Finding identified as an internal control deficiency should be categorized as either a Material Weakness or a Reportable Condition based on the following definitions:

• A **Reportable Condition** exists when the internal controls are adequate in design and operation and reasonable assurance can be provided that the intent of the

control objective is met, but deficiencies were found during the review that requires correction.

• A **Material Weakness** exists when the contractor fails to meet a control objective. This may be due to a significant deficiency in the design and/or operation of internal control policies and procedures. Because of these shortfalls in internal controls, the contractor cannot provide reasonable assurance that the intent of the control objective is being met.

2.8.1.6 Finding Security Control Family

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All Findings *shall* be assigned to one of the *CMS Security Control Families*. These *families* are available from a drop-down menu in the CISS.

2.8.1.7 Finding Point(s) of Contact

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

For each Finding reported, a primary POC *shall* be selected. While multiple POCs can be assigned to a Finding, only one POC can be designated as primary for each Finding. The primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the Finding. Non-primary POCs can include anyone who will assist the primary POC in resolving the Finding.

2.8.2 Weaknesses

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All security-related Weaknesses identified by internal or external audits and reviews, including *FISMA Evaluations*, *shall* be entered into the CISS and associated with (i.e., linked to) an Action Plan AND one or more Findings.

The following subsections provide guidance for populating the CISS Weakness form. Consult the CISS User Guide for specific instructions related to accessing and working with CISS Weakness form components.

2.8.2.1 Weakness Identifier

(*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

Each Weakness *shall* be identified and recorded by a unique identifier consisting of the following information:

a) **Entity.** The first three *(3) to five (5)* characters identify the name of the contractor. These contractor *identifiers* are listed under contractor abbreviations in Chapter 7, Internal Control Requirements, section 40.3, CMS Finding Numbers, of the Medicare Financial Manual.

NOTE: This unique contractor identifier is not reported or included in CMS' annual or quarterly POA&M submissions. Therefore, Weaknesses reported outside CMS cannot be traced to a *CMS organization or contractor* by any information included in the Weakness identifier.

b) **Quarter.** The next single character represents the FY quarter in which the Weakness was first identified and entered into the POA&M, where:

A = 1st QuarterB = 2nd QuarterC = 3rd QuarterD = 4th Quarter

- c) Year. The next four (4) digits are the FY in which the Weakness was identified and first reported.
- d) **Number.** The next number is incremental, representing the sequence in which the Weakness was entered into the contractor's POA&M.

For example, a Weakness identified as "CMS_B_2005_3" indicates this CMS Weakness was identified and first reported during the 2nd quarter of FY 2005, and it is the 3rd Weakness identified during that time period.

2.8.2.2 Weakness Title and Description

(*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

The Weakness title *shall* not include any contractor-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the contractor reporting the Weakness, which location or facility has the Weakness, or what system or application has the Weakness.

The intent is to provide a title that is descriptive but does not reveal sensitive or exploitable information. The title *shall* also be unique enough to be more readily identifiable by name than by number.

The Weakness description, however, is not reported beyond CMS, and it *shall* provide sufficient information and detail to allow CMS to evaluate the Weakness.

2.8.2.3 Weakness Security Control Family (*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

All Weaknesses *shall* be assigned to one of the *CMS Security Control Families*. These *families* are available from a drop-down menu in the CISS:

2.8.2.4 Determination of Weakness Risk Level

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

System Weakness risk levels should be determined in the system's risk assessment according to criteria in the CMS *IS* RA *Procedures*.

2.8.2.5 Weakness FISMA Severity

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

FISMA requires the reporting of any significant deficiency in a policy, procedure, or practice to be identified as a material Weakness under the Federal Managers Financial Integrity Act (FMFIA), and if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (FFMIA). Depending on the risk and magnitude of harm that could result, Weaknesses identified during the review of security controls are reported as deficiencies in accordance with OMB Circular No. A 123, "Management Accountability and Control," and FMFIA.

Although the CISS includes the three (3) FISMA Severity levels listed below, only one (1) level is activated and available for use by *organizations* (i.e., Weakness). The other two (2) severity levels, Significant Deficiency and Reportable Condition, require that CMS make a risk-based decision before a Weakness can be assigned to them. Should CMS make that determination, additional guidance will be provided on how to select a different severity level.

The three (3) FISMA Severity levels are:

• **Weakness.** The term Weakness refers to any and all other IT security Weaknesses pertaining to the system.

NOTE: This is the only severity level that can be selected by *organizations* at this time.

• **Reportable Condition.** A Reportable Condition exists when a security or management control Weakness does not rise to a significant level of deficiency; yet, it is still important enough to be reported to internal management. A security Weakness may be considered a Reportable Condition even though it is not deemed to be a Significant Deficiency by agency management if it affects the

efficiency and effectiveness of agency operations. However, due to lower risk, corrective action may be scheduled over a longer period of time.

• **Significant Deficiency**. A Significant Deficiency exists when a Weakness in an agency's (i.e., CMS) overall information systems security program or management control structure, or within one or more information systems, significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies *shall* be notified and immediate or near-immediate corrective action *shall* be taken.

2.8.2.6 Weakness Type

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

There are two (2) types of security-related Weakness that *shall* be identified:

- **Program Weakness.** A Program Weakness impacts multiple IT systems as a result of a deficiency in the IT security program.
- **System Weakness.** A System Weakness pertains to the management, operation, or technical controls of a specific IT system.

2.8.2.7 Weakness Status

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All security-related Weakness corrective actions *shall* include a status that indicates the stage or state of the Weakness corrective action. Since multiple Findings may be associated with a Weakness, the Weakness cannot be closed until all Findings associated with it are closed. The five (5) Weakness status reporting choices are:

- **On-going.** The Weakness remains open and action is on-going to correct it. However, if the Initial Target Completion Date entered in the Action Plan has passed and action is still on-going to correct the Weakness, the status *shall* be reported as Delayed.
- Closed Pending. (1) If the Weakness was discovered in an internal review, the organization may proceed directly to the Closed status. (2) If the Weakness was discovered in an outside audit or review, the organization should use this status when it considers the Weakness closed. However, CMS requires this type of Weakness closure to be validated before it is considered closed. The contractor should continue to report the status as Closed Pending until the closure is validated.

- **Closed.** If a Weakness has been officially closed by *CMS*, with supporting documentation as proof submitted to the organization, it should be reported as *Closed in the CISS*.
- **Delayed.** Action is on-going to correct the Weakness but the Initial Target Completion Date entered in the Action Plan has passed. The Weakness should continue to be reported as Delayed until the Weakness is corrected and reported as closed.

2.8.2.8 Weakness Point(s) of Contact

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

For each Weakness identified, a primary POC *shall* be selected. While multiple POCs can be assigned to a Weakness, only one POC can be designated as primary for each Weakness. The primary POC is the individual whose position/role (e.g., SSO, system owner, system administrator) is ultimately responsible for resolving the Weakness. Non-primary POCs can include anyone who will assist the primary POC in resolving the Weakness.

2.8.2.9 Determining Risk

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The risk determination process explained in this section is taken from the CMS IS RA *Procedures*. The process described here assumes that specific threats and vulnerabilities have already been identified. Consult the CMS IS RA *Procedures* for specifics on identifying threats and vulnerabilities.

While both system and business risk measurements are discussed and combined in the CMS IS RA *Procedures* document, risk determinations made in and by the CISS are for systems only. The goal of risk determination is to calculate the level of risk for each threat/vulnerability pair based on:

- 1. The likelihood of a threat exploiting a vulnerability; and
- 2. The severity of impact that the exploited vulnerability would have on the system, its data and its business function in terms of loss of CIA.

2.8.2.9.1 Likelihood of Occurrence

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The risk likelihood level is determined by considering known threats as they may apply to known system vulnerabilities. The likelihood is an estimate of the frequency or the probably of such an event. The likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access, and existing controls; the presence, motivation, tenacity, strength, and nature of the threat; the presence of vulnerabilities; and the effectiveness of existing controls. Refer to the information in Table A- $\frac{8}{8}$ for guidelines to determine the likelihood of occurrence that a threat is realized and exploits the system's vulnerability.

Likelihood	Description
Negligible	Unlikely to occur.
Very Low	Likely to occur two (2) /three (3) times every five (5) years.
Low	Likely to occur once every year or less.
Medium	Likely to occur once every six (6) months or less.
High	Likely to occur once per month or less.
Very High	Likely to occur multiple times per month.
Extreme	Likely to occur multiple times per day.

Table A-8. Likelihood of Occurrence Levels

2.8.2.9.2 Impact Severity

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The severity of impact is the magnitude or severity of impact on the system's operational capabilities and data if the threat is realized and exploits the associated vulnerability. The severity of impact for each threat/vulnerability pair is determined by evaluating the potential loss in each security category (CIA) based on the system's information security level as explained in BPSSM Section 4.0, Information and Information Systems Security. The impact can be measured by loss of system functionality, degradation of system response time, or inability to meet a CMS business function, dollar losses, loss of public confidence, or unauthorized disclosure of data.

Refer to Table A-9 for guidelines to determine system impact severity levels.

Impact Severity	Description	
Insignificant	Will have almost no impact if threat is realized and exploits vulnerability.	
MinorWill have some minor effect on the system. It will require min effort to repair or reconfigure the system.		
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.	
DamagingMay cause damage to the reputation of system management notable loss of confidence in the system's resources or servi will require expenditure of significant resources to repair.		
Serious May cause considerable system outage, and/or loss of connect		

Table A-9. System Impact Severity Levels

Impact Severity	Description	
	customers or business confidence. May result in compromise or large amount of Government information or services.	
Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.	

2.8.2.9.3 Determining the Risk Level (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The overall risk level can be expressed in terms of the likelihood of the threat exploiting the system vulnerability and the impact severity of that exploitation on the CIA of the system. This overall level of risk is depicted in the following equation:

Risk Level = Likelihood of Occurrence X Impact Severity

After the risk likelihood of occurrence and impact severity have been established, the overall level of risk is determined using the following risk level matrix (Table A-10). The level of risk equals the intersection of the likelihood of occurrence and impact severity values. The CISS determines this value automatically based on the input values of the Weakness likelihood of occurrence and impact severity selections.

Likelihood	Impact Severity					
of Occurrence	Insignificant	Minor	Significant	Damaging	Serious	Critical
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

 Table A-10. Overall Risk Level Matrix

2.9 Action Plans and POA&Ms

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Action Plans form the basis for the periodic POA&M reporting requirement (see section 3.5.2 of the BPSSM for reporting requirements).

The CISS assists *organizations* in reporting Weaknesses, preparing Action Plans, and submitting the required POA&Ms to CMS. The POA&M submission process is

automatic in that it contains information already entered into the CISS. Therefore, no further guidance is required beyond the instructions found in section 11, Submissions to CMS, of the CISS User Guide. The remainder of this section is devoted to guidance for populating the CISS Action Plan form.

2.9.1 Completing Action Plans

(*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

Each Weakness entered into the CISS *shall* correspond to an Action Plan for its resolution. Although the CISS does permit multiple Weaknesses to be addressed by a single Action Plan, this approach is not recommended, because a Weakness cannot be closed until its corresponding Action Plan has been completed.

Corrective action methods should be analyzed for appropriateness in fully resolving any associated Weakness; they should also be viewed for long-term implications. When completing an Action Plan, the cost for each option *shall* be estimated and analyzed to determine short- and long-term solution capabilities.

2.9.1.1 Action Plan Title and Description

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Action Plan title *shall* not include any contractor-, location-, or system-specific information, or other sensitive or identifying information. Otherwise, the title information could be used to identify the contractor reporting the Weakness, which location or facility has the Weakness, or what system or application has the Weakness. The title is used only to provide a descriptive name to the Action Plan so it can be distinguished from other Action Plans.

Detailed descriptions of Action Plans are necessary, and sufficient text is required to permit oversight and tracking. Sensitive information *shall* not be revealed in the description of the Action Plan, Weakness, or associated Milestones. In addition, no contractor-, location-, or system-specific information *shall* be included in the Action Plan description. Otherwise, the descriptive information can be used to identify the contractor, location or facility, or system or application.

2.9.1.2 Determining Completion Dates

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Completion Dates (i.e., Initial Target, Current Projected, and Actual) are populated automatically based on dates entered in the Milestones. These dates will change based on the Milestone dates until the Action Plan is reported in a POA&M submission. Once the Action Plan has been initially submitted to CMS, the Initial Target date is locked and cannot be changed. So, when completing Milestones, completion dates *shall* be determined based on realistic timelines for resources to be obtained and associated steps to be completed. For example, although it may take 30 days to complete the required Action Plans for a specific Weakness, it may not be possible to complete ALL Action

Plans for all Weaknesses during the same time period due to staffing resource limitations. Therefore, the Initial Target Milestone dates *shall* be based on the outcome of prioritization decisions and resource availability.

2.9.1.3 Determining Costs

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

In determining Weakness remediation costs, *organizations shall* consider the following criteria to determine security costs for a specific IT investment:

- a) The products, procedures, and personnel (*organization* employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. This includes the costs of:
 - Risk assessment
 - Security planning and policy
 - Certification and accreditation
 - Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
 - Authentication or cryptographic applications
 - Education, awareness, and training
 - System reviews/evaluations (including security control testing and evaluation)
 - Oversight or compliance inspections
 - Development and maintenance of *organization* reports to CMS and corrective Action Plans as they pertain to the specific investment
 - Contingency planning and testing
 - Physical and environmental controls for hardware and software
 - Auditing and monitoring
 - Computer security investigations and forensics
 - Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations
- b) Security costs *shall* also include the products, procedures, and personnel (*organization* employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; system administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.
- c) Many corporate entities operate networks that provide some or all of the necessary security controls for the associated applications. In such cases, the *organization shall* nevertheless account for security costs for each application investment. To avoid "double-counting," *organizations* should appropriately

allocate the costs of the network for each of the applications for which security is provided.

In identifying security costs, *organizations* may find it helpful to ask the following simple question: "If there were no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" If *organizations* encounter difficulties with the above criteria, they *shall* contact CMS prior to submission of their POA&M report.

Target Implementation Costs are the total costs for implementing the remediation safeguards during the first year of implementation. This *shall* include purchases, leases, setup and delivery, consultant services, applicable overhead, depreciation, amortization, cost of money, and all other associated costs in accordance with disclosure practices. Since this cost may be used for budgetary purposes, it *shall* be as accurate as feasible. It is advised that finance, accounting, or other personnel familiar with the application of cost estimating practices be consulted when estimating this cost.

The Estimated Annual Maintenance cost is the projected recurring cost of implementing the remediation safeguards. This is the projected recurring cost to CMS to maintain this remediation safeguard for the following FY. This cost *shall* include depreciation, amortization, etc. Costs associated with continued funding should be added to subsequent line one charges where applicable.

The Percent Security value is the percentage of the total remediation safeguard costs that pertain or apply to security.

The Percent Applied to CMS is the percentage of the total remediation safeguard cost being charged to CMS. This is the percentage of cost that CMS will fund for safeguards that will be shared between CMS (Medicare) systems and corporate systems.

2.9.1.4 Determining Funding Sources

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CISS requires that some resources be identified for every Action plan. Action Plans cannot be executed without the application of resources (personnel or procurement). Therefore, the CISS will not accept "zero-cost" Action Plans. Resources for Weakness remediation can be obtained through the following means:

- Using current resources marked for security management of the system or program. This *shall* be the method used for resourcing most Weaknesses.
- Reallocating existing funds or personnel.
- Requesting additional funding.

Requesting new or additional funding from CMS to remediate a Weakness should only be used when no other source of funding can be identified. When funding is available, CMS will prioritize funding allocations based on Weakness prioritization and risk levels. It is in the *organization*'s best interest to use current resources or reallocate existing funds or personnel to remediate all Weaknesses. All funding reallocations *shall* be approved by CMS.

2.9.1.5 Milestone Title and Description

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Milestone title *shall* not include any sensitive or identifying information. The title *shall* be descriptive enough to distinguish one Milestone from another.

Detailed descriptions of Milestones are not necessary, but sufficient data is required to permit oversight and tracking. Sensitive or identifying information *shall* not be revealed in the Milestone descriptions.

2.9.1.6 Milestones with Completion Dates

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Fundamentally, the Action Plan is simply a container for the Milestones that address remediation of any corresponding Weakness. The Milestones are identified in the POA&M, and each one *shall* correspond to a specific corrective action. Ideally, there *shall* be at least one Milestone per quarter so that Action Plan progress can be tracked in the POA&M submissions to CMS.

Including anticipated completion dates with each Milestone enables progress toward Weakness mitigation to be tracked. Each Milestone within the POA&M *shall* include an anticipated date of completion (Projected Date). Once Milestones and completion dates are entered, changes can be made until the Action Plan is first submitted.

The overall projected completion date of the Action Plan is derived automatically by the CISS based on the projected completion dates of all of the Milestones. The Initial Target date remains unchanged once the Action plan has been submitted to CMS. However, the Current Projected Date will adjust automatically based on changes in milestone projected completion date. (Note that the Action Plan status of "Delayed" is always calculated based on the Initial Target date.)

Milestones should effectively communicate the major steps within an Action Plan that *shall* be performed to mitigate a Weakness. For example, appropriate Milestones for an Action Plan associated with a Weakness such as "Identification and authentication process need to be more stringent" might read:

- Evaluate methods for strengthening identification and authentication
- Develop procedures to standardize accepted authentication process
- Acquire management approval/sign-off of new process and procedures
- Implement approved authentication process

2.9.1.7 Milestone Changes

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

If a situation exists that prevents a Milestone and/or overall corrective action from being completed on time, the new estimated date of completion will automatically be reflected in the Current Projected date based on the Milestone changes. However, once the Action Plan has been submitted, the Initial Target date field is locked and cannot be changed. Any changes to a Milestone *shall* include the reason(s) for the delay.

Business Partners Systems Security Manual

Appendix A, Attachment 1

CMS Core Security Requirements (CSR)

for

High Impact Level Assessments



CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

Rev. 9

(This page intentionally left blank)

Access Control (AC) – Technical

AC-1 – Access Control Policy and Procedures (High)

Control

Logical access controls and procedures shall be established and implemented effectively to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (i.e., programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

Guidance

The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applic	References: ARS: AC-1; FISCAM: TAC-3.2.C.1, TAC-4.3.4, TSD-1.1.1, TSD-2.1, TSS-1.1.1; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1; NIST 800-53/53A: AC-1; PISP: 4.1.1	Related Controls:

ASSESSMENT PROCEDURE: AC-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents access control policy and procedures;

(ii) the organization disseminates access control policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review access control policy and procedures; and

(iv) the organization updates access control policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities.

ASSESSMENT PROCEDURE: AC-1.2

Assessment Objective

Determine if:

(i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

- (ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
- (iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities.

AC-1(FIS-1) – Enhancement (High)

Control

Standard forms are used to document approval for archiving, deleting, or sharing data files. Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

Applicability: All	References: FISCAM: TAC-2.3.1, TAC-2.3.2	Related Controls:
ASSESSMENT PROCEDURE: AC-1(FIS-1).1		

Assessment Objective

Determine if:

(i) the organization uses standard forms to document approval for archiving, deleting, or sharing data files; and

(ii) the organizational agreements, with other entities, document prior to sharing data or programs how the data files are protected.

Assessment Methods And Objects

Examine: Documents authorizing file sharing and file sharing agreements.

Examine: Pertinent policies and procedures.

Examine: Standard approval forms.

Interview: Data owners.

AC-2 – Account Management (High)

Control

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. Access to the CMS information system shall be granted based on: (a) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (b) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

Guidance

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system usage or need-to-know/need-to-share changes.

Applicability: All	References: ARS: AC-2; FISCAM: TAC-3.2.C.4, TAC-3.2.C.5, TSP-4.1.6, TSS-1.1.3; HIPAA:	Related Controls:
	164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1; NIST 800-	
	53/53A: AC-2; PISP: 4.1.2	
	•	

ASSESSMENT PROCEDURE: AC-2.1

Assessment Objective

Determine if:

(i) the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts;

(ii) the organization defines the frequency of information system account reviews;

(iii) the organization reviews information system accounts at the organization-defined frequency, at least annually; and

(iv) the organization initiates required actions on information system accounts based on the review.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing account management; information system security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities.

interview. Organizational persor					
AC-2(0) – Enhancement (High)					
Control					
Review information system acco	unts every 90 days and require annual certification.				
Applicability: All	References: ARS: AC-2(0); FISCAM: TAC-3.2.C.4, TSS-1.1.4; HIPAA: 164.308(a)(3)(ii)(B),	Related Controls:			
	164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2				
ASSESSMENT PROCEDURE: A	C-2(0).1				
Assessment Objective					
Determine if the organization me	ets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amp	blifying enhancement to the baseline control.			
Assessment Methods And Objects					
Examine: Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list					
of recently separated or terminat	ed employees; list of recently disabled information system accounts; system-generated records with user IDs and las	t login date; other relevant documents or			
records.					

Interview: Organizational personnel with account management responsibilities.

AC-2(1) – Enhancement (High)				
Control				
Employ automated mechanisms to support the management of information system accounts.				
Applicability: All References: ARS: AC-2(1); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(1) Related Controls:				

ASSESSMENT PROCEDURE: AC-2(1).1				
Assessment Objective				
	d mechanisms to support information system account management functions.			
issessment Methods And Objects				
	agement; information system design documentation; information system configuration settings	s and associated documentation: other relevant		
documents or records.				
Test: Automated mechanisms implementing ac	count management functions.			
AC-2(2) – Enhancement (High)				
Control				
	gency account for a period of time NTE 24 hours and to allow accounts with a fixed duration (i.	e temporary accounts) NTE 365 days		
Applicability: All	References: ARS: AC-2(2); FISCAM: TAC-2.2; IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: A			
ASSESSMENT PROCEDURE: AC-2(2).1				
Assessment Objective				
	hich the information system terminates temporary and emergency accounts; and			
	tes temporary and emergency accounts after organization-defined time period for each type o	of account		
Assessment Methods And Objects				
	rmation system design documentation; information system configuration settings and associa	ted documentation: information system audit records:		
other relevant documents or records.	and do by stem design dood ner dation, information by stem coninguration bettings and dooold			
Test: Automated mechanisms implementing act	count management functions.			
AC-2(3) – Enhancement (High)				
Control				
Configure the information system to disable inac	tive accounts automatically after 90 days			
Applicability: All	References: ARS: AC-2(3); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.2#2.1; NIST 800-53/53.	A: AC-2(3) Related Controls: IA-4(0)		
ASSESSMENT PROCEDURE: AC-2(3).1				
Assessment Objective				
Determine if:				
	hich the information system disables inactive accounts; and			
(ii) the information system automatically disables inactive accounts after organization-defined time period.				
Assessment Methods And Objects				
Examine: Procedures addressing account management; information system security plan; information system design documentation; information system configuration settings and associated				
documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records.				
Test: Automated mechanisms implementing ac				
AC-2(4) – Enhancement (High)				
Control				
	count creation, modification, disabling, and termination. Ensure the automated mechanism n	otifies appropriate personnel of the user account		
management actions.				
Applicability: All	References: ARS: AC-2(4); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(4)	Related Controls:		
ASSESSMENT PROCEDURE: AC-2(4).1				
Assessment Objective				
Determine if:				
	isms to audit account creation, modification, disabling, and termination actions; and			
	nisms to notify, as required, appropriate individuals.			
Assessment Methods And Objects				
	agement; information system design documentation; information system configuration settings	s and associated documentation; information system		
audit records; other relevant documents or reco				
Test: Automated mechanisms implementing ac				
Rev. 9	Page 3 of 207	BPSSM Appendix A, Attachment 1		
	-	* *		

AC-2(CMS-1) – Enhancement (High	lh)		
Control	_		
Remove or disable default user acco	ounts. Rena		
Applicability: All		References: ARS: AC-2(CMS-1); FISCAM: TAC-3.2.A.3, TAC-3.2.C.4, TSS-1.2.3; IRS-1075: 5.6.3.2#2.1	Related Controls:
ASSESSMENT PROCEDURE: AC-2	2(CMS-1).	1	
Assessment Objective			
Determine if the organization manac	ges informat	ion system accounts, including establishing, activating, modifying, reviewing, disabling, and removi	ng accounts.
Assessment Methods And Objects	S		
1, ,	d procedures	s; other relevant documents or records to determine if the organization removes or disables default	user accounts. It must also rename active default
accounts if they must be used.			
renamed.		s control responsibilities to determine that all default user accounts are either removed or disabled.	
		defined users to ensure that all default user accounts are either removed or disabled. If default acc	ounts are active, that they are renamed.
AC-2(CMS-2) – Enhancement (Higl	h)		
Control			
Require the use of unique and sepa	arate adminis	strator accounts for administrator and non-administrator activities.	
Applicability: All		References: ARS: AC-2(CMS-2); FISCAM: TAN-2.1.4; IRS-1075: 5.6.3.2#2.1	Related Controls: IA-4(CMS-1)
ASSESSMENT PROCEDURE: AC-2	2(CMS-2).	1	
Assessment Objective			
Determine if the information system	enforces se	paration of duties through assigned access authorizations.	
Assessment Methods And Objects	S		
		gement procedures; information system security plan (for organization-defined account review frequence)	
		list of recently disabled information system accounts; system-generated records with user IDs and	last login date; other relevant documents or records
• •		strator accounts to be used for day-to-day activities.	
		Int management responsibilities to determine if administrator accounts are being used for day to da m logs to ensure that administrator accounts are not being used for day-to-day activities.	y activities.
AC-2(CMS-3) – Enhancement (High			
	µ1)		
Control		Iniziatestas functiona	
Implement centralized control of use Applicability: All	er access ac	References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1	Related Controls:
ASSESSMENT PROCEDURE: AC-2	2/CME 2)		Related Controls.
	2(010-3).		
Assessment Objective	ann informal	ion system accounts including actablishing, activating madifying, reviewing, disabling, and remay	ng occounto
Assessment Methods And Objects		ion system accounts, including establishing, activating, modifying, reviewing, disabling, and removi	ng accounts.
Assessment Methous And Objects	3		
Examine: Access control policy: acc	count mana	gement procedures: information system security plan (for organization-defined account review frequ	uency): list of active user and system accounts: list
		gement procedures; information system security plan (for organization-defined account review frequentiation system accounts; system-generated records with user IDs and	
	employees;	list of recently disabled information system accounts; system-generated records with user IDs and	
of recently separated or terminated of to determine if all user access admir	employees; nistrator fun	list of recently disabled information system accounts; system-generated records with user IDs and	last login date; other relevant documents or records
of recently separated or terminated of to determine if all user access admir Interview: Organizational personnel	employees; nistrator fun el with accou	list of recently disabled information system accounts; system-generated records with user IDs and ctions are centralized.	last login date; other relevant documents or records ut by a centralized administrator function.
of recently separated or terminated of to determine if all user access admir Interview: Organizational personnel	employees; nistrator fun el with accou hosts' syste	list of recently disabled information system accounts; system-generated records with user IDs and ctions are centralized. Int management responsibilities to determine if all user access administrator functions are carried o	last login date; other relevant documents or records ut by a centralized administrator function.
of recently separated or terminated of to determine if all user access admir Interview: Organizational personnel Test: Information system sample of	employees; nistrator fun el with accou hosts' syste	list of recently disabled information system accounts; system-generated records with user IDs and ctions are centralized. Int management responsibilities to determine if all user access administrator functions are carried o	last login date; other relevant documents or records ut by a centralized administrator function.
of recently separated or terminated of to determine if all user access admir Interview: Organizational personnel Test: Information system sample of AC-2(CMS-4) – Enhancement (High Control	employees; nistrator fun el with accou hosts' syste h)	list of recently disabled information system accounts; system-generated records with user IDs and ctions are centralized. Int management responsibilities to determine if all user access administrator functions are carried o	last login date; other relevant documents or records ut by a centralized administrator function.

ASSESSMENT PROCEDURE: AC-2(CMS-4).1

Assessment Objective

Determine if the organization documents contractor security requirements and maintains contractor access privileges.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if all contractors' access are authorized, regulated, and security requirements for contractors are defined.

Interview: Organizational personnel with account management responsibilities to determine if written authorizations exist for a sample of contractor employees.

AC-2(CMS-5) – Enhancement (High)

Control

Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked prior to or during the termination process.

Applicability: All	References: ARS: AC-2(CMS-5); FISCAM: TSP-4.1.6; IRS-1075: 5.6.3.2#2.1	Related Controls:
ASSESSMENT PROCEDURE: AC-2(CMS-5) 1		

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Access control policy; account management procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine when employee access rights are revoked on termination.

Interview: Organizational personnel with personnel security responsibilities to determine when access is revoked on employee termination.

AC-2(FIS-1) – Enhancement (High)

Control

All system access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to security managers.

Guidance

The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties.

Applicability: All	References: FISCAM: TAC-2.1.1, TAC-2.2	Related Controls:

ASSESSMENT PROCEDURE: AC-2(FIS-1).1

Assessment Objective

Determine if:

(i) the organization grants system access authorizations on standard forms and maintains the completed forms on file; and

(ii) the organizational senior managers approve system access authorizations and the approvals are securely transferred to security managers.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Selection of user (both application user and information system personnel) access authorization documentation.

Interview: Personnel involved in access authorizations and senior managers who approve authorizations.

AC-2(FIS-2) – Enhancement (High)

Control

Business Owners periodically review system access authorization listings and determine whether they remain appropriate. ISSO/SSOs review system access authorizations and discuss any questionable authorizations with Business Owners.

Applicability: All	References: FISCAM: TAC-2.1.2, TAC-2.1.4	Related Controls:

ASSESSMENT PROCEDURE: AC-2(FIS-2).1

Assessment Objective

Determine if the organizational ISSO/SSOs periodically reviews system access authorization listings and discusses questionable authorizations with management.

Assessment Methods And Objects

Examine: Access authorization listings to determine whether inappropriate access are removed in a timely manner.

Examine: Pertinent policies and procedures.		
Interview: Business Owners and review support	rting documentation. Determine whether inappropriate access is removed in a timely manner.	
Interview: ISSO/SSOs and review documentat	ion provided to them.	
AC-3 – Access Enforcement (High)		
Control		
in a CMS information system. Additional applic	eloped, documented and implemented effectively to control access between named users (or processes) a ation level access enforcement mechanism shall be implemented, when necessary, to provide increased yed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (s	information security for CMS information.
Guidance		<i>i</i>
cryptography) are employed by organizations to information system. In addition to controlling ac information security for the organization. Consid	icies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., acc o control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, r cess at the information system level, access enforcement mechanisms are employed at the application le deration is given to the implementation of a controlled, audited, and manual override of automated mechan on is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended	ecords, processes, programs, domains) in the vel, when necessary, to provide increased nisms in the event of emergencies or other
Applicability: All	References: ARS: AC-3; FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.C.6, TAC-3.2.D.1, TCC-3.2.3, TSS-2.1.1, TSS-2.1.2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3; NIST 800-53/53A: AC-3; PISP: 4.1.3	Related Controls: MA-CMS-1, MA-CMS-2, SC-13
ASSESSMENT PROCEDURE: AC-3.1		
 (ii) user privileges on the information system are Assessment Methods And Objects Examine: Access control policy; procedures ad privileges); information system audit records; ot Test: Automated mechanisms implementing ac AC-3(1) – Enhancement (High) Control 	cess enforcement policy. to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardw	
1 7	inorized individuals.	
	nple, security administrators, system and network administrators, and other privileged users. Privileged us nctions (e.g., system administrators, information system security officers, maintainers, system programme	
Applicability: All	References: ARS: AC-3(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.2, TAC-3.2.C.5, TAC-3.2.D.1, TCC- 3.2.3, TSD-3.1.4, TSS-1.1.2, TSS-2.1.2; IRS-1075: 5.6.3.2#2.2; NIST 800-53/53A: AC-3(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-3(1).1		
Assessment Objective Determine if:		

Test: Automated mechanisms implementing access enforcement policy.

AC-3(CMS-1) – Enhancement (High)

Control

If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

	Applicability: All	References: ARS: AC-3(CMS-1); IRS-1075: 5.6.3.2#2.2	Related Controls: SC-13
ASSESSMENT PROCEDURE: AC-3(CMS-1).1			

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if encryption is used as an access control mechanism, examine system and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Interview: Organizational personnel with access control responsibilities to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Test: Information system if encryption is used as an access control mechanism; examine organization's encryption key lengths, algorithms, certificates, etc.

AC-3(CMS-2) – Enhancement (High)

Control

If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix A for e-Authentication Standards.

Applicability: All	References: ARS: AC-3(CMS-2); IRS-1075: 5.6.3.2#2.2	Related Controls:
ASSESSMENT PROCEDURE: AC-3(CMS-2).1		

Assessment Objective

Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if e-authentication is used as an access control mechanism, examine Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the organization's encryption standard meets ARS Appendix A for e-Authentication Standards.

Interview: Organizational personnel with access control responsibilities if e-authentication is used as an access control mechanism, interview system administrators responsible for the hosts providing authentication services to determine if the organization meets the standards described in ARS Appendix A.

Test: Information system if e-authentication is used as an access control mechanism; test a sample of hosts for automated mechanisms implementing identification and authentication capability for the information system.

AC-3(CMS-3) – Enhancement (High)

Control

Configure operating systems controls to disable public "read" and "write" access to all system files, objects, and directories. Configure operating system controls to disable public "read" access to files, objects, and directories that contain sensitive information.

Applicability: All	References: ARS: AC-3(CMS-3); FISCAM: TAC-3.2.D.1, TCC-3.2.3; IRS-1075: 5.6.2.3#1,	Related Controls:	
	5.6.3.2#2.2		
ASSESSMENT PROCEDURE: AC-3(CMS-3).1			

Assessment Objective

Determine if the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive

information.

Interview: Organizational personnel with access control responsibilities to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

Test: Automated mechanisms implementing access enforcement policy to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

AC-3(CMS-4) – Enhancement (High) Control Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas.

Applicability: All	References: ARS: AC-3(CMS-4); FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.D.1, TAY-3.1.6, TCC-3.2.3; HIPAA: 164.312(a)(2)(iv); IRS-1075: 5.6.3.2#2.2	Related Controls:

ASSESSMENT PROCEDURE: AC-3(CMS-4).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if data stored in the information system is protected with system access controls and must be encrypted when residing in non-secure areas.

Interview: Organizational personnel with access control responsibilities to determine if hosts storing data are protected with system access controls and if data stored in non-secure areas are encrypted.

Test: Automated mechanisms implementing access enforcement policy to if data stored on these hosts is protected with system access controls and that it is encrypted if residing in non-secure areas.

AC-4 – Information Flow Enforcement (High)

Control

Flow control shall be enforced over information between source and destination objects within CMS information systems and between interconnected systems based on the characteristics of the information.

Guidance

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

Applicability: All	References: ARS: AC-4; IRS-1075: 5.6.3.2#2.2; NIST 800-53/53A: AC-4; PISP: 4.1.4	Related Controls: SC-7
ASSESSMENT PROCEDURE: AC-4.1		

Assessment Objective

Determine if the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records. **Test:** Automated mechanisms implementing information flow enforcement policy.

ASSESSMENT PROCEDURE: AC-4.2

Assessment Objective

Determine if interconnection agreements address the types of permissible and impermissible flow of information between information systems and the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system interconnection agreements; information system configuration settings and associated

documentation; list of information flow	v control authorizations; information system audit records; other relevant documents or records.	
AC-5 – Separation of Duties (Hi		
Control		
support functions shall be divided amond also administer audit functions).	shall be enforced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission ong different roles, and support functions shall be performed by different individuals (e.g., personnel responsible fo Personnel developing and testing system code shall not have access to production libraries. Access control softwa	r administering access control functions shall are shall be in place to limit individual authority
	collusion of two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurat	ely the assigned duties and responsibilities
that support separation of duties.		
The organization establishes appropri control software on the information sy of duties include: (i) mission functions	iate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities /stem that prevents users from having all of the necessary authority or information access to perform fraudulent act and distinct information system support functions are divided among different individuals/roles; (ii) different individ systems programming, quality assurance/testing, configuration management, and network security); and (iii) secur tions.	ivity without collusion. Examples of separation uals perform information system support
Applicability: All	References: ARS: AC-5; FISCAM: TAY-1.3.2, TSD-1.1.1, TSD-1.1.2, TSD-1.1.3, TSD-1.1.5, TSD-1.2.1, TSD-1.3.3, TSD-2.2.2, TSS-1.1.2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3; NIST 800-53/53A: AC-5; PISP: 4.1.5	Related Controls:
ASSESSMENT PROCEDURE: AC-5.	1	
Assessment Objective		
Determine if:		
(i) the organization establishes approp(ii) the information system enforces set	priate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilit eparation of duties through assigned access authorizations.	ies and duties of individuals; and
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; proc information system audit records; othe Interview: Organizational personnel v 	eparation of duties through assigned access authorizations. redures addressing separation of duties; information system configuration settings and associated documentation; er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties.	
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; proc information system audit records; othe Interview: Organizational personnel v Test: Automated mechanisms implem 	eparation of duties through assigned access authorizations. redures addressing separation of duties; information system configuration settings and associated documentation; er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy.	
 (i) the organization establishes appropriate (ii) the information system enforces set Assessment Methods And Objects Examine: Access control policy; process information system audit records; other information system audit records; other interview: Organizational personnel votational personnel votational personnel votational methanisms implem AC-5(CMS-1) – Enhancement (High) 	eparation of duties through assigned access authorizations. redures addressing separation of duties; information system configuration settings and associated documentation; er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy.	
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; procinformation system audit records; other Interview: Organizational personnel v Test: Automated mechanisms implem AC-5(CMS-1) – Enhancement (High) Control 	eparation of duties through assigned access authorizations. redures addressing separation of duties; information system configuration settings and associated documentation; er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy.	
 (i) the organization establishes appropriate (ii) the information system enforces set Assessment Methods And Objects Examine: Access control policy; prociniformation system audit records; other information system audit records; other information system audit personnel with the transmission of transmission of the transmission of tr	eparation of duties through assigned access authorizations. redures addressing separation of duties; information system configuration settings and associated documentation; l er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy.) erformed by security personnel responsible for administering access control.	
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; proci information system audit records; othe Interview: Organizational personnel v Test: Automated mechanisms implem AC-5(CMS-1) – Enhancement (High) Control Ensure that audit functions are not pe Applicability: All 	eparation of duties through assigned access authorizations. redures addressing separation of duties; information system configuration settings and associated documentation; l er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy.) erformed by security personnel responsible for administering access control. References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5	list of separation of duties authorizations;
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; procinformation system audit records; other Interview: Organizational personnel w Test: Automated mechanisms implem AC-5(CMS-1) – Enhancement (High) Control Ensure that audit functions are not pe Applicability: All ASSESSMENT PROCEDURE: AC-5(Assessment Objective Determine if the organization establisi 	eparation of duties through assigned access authorizations. redures addressing separation of duties; information system configuration settings and associated documentation; l er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy.) erformed by security personnel responsible for administering access control. References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5	list of separation of duties authorizations;
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; procinformation system audit records; other Interview: Organizational personnel with the terview: Organization and the terview: Organization and the terview: Organization applicability: All Assessment Objective Determine if the organization establish Assessment Methods And Objects Examine: Separation of duties policy records; other relevant documents or enforces separation of duties through 	eparation of duties through assigned access authorizations. eedures addressing separation of duties; information system configuration settings and associated documentation; if er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy. erformed by security personnel responsible for administering access control. References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5 (CMS-1).1 hes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the re and procedures; information system configuration settings and associated documentation; list of separation of dutie records to determine if audit functions are NOT performed by security personnel responsible for administering access authorizations.	list of separation of duties authorizations; Related Controls: sponsibilities and duties of individuals. ies authorizations; information system audit ess control. Also, ensure that the organization
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; proci- information system audit records; other Interview: Organizational personnel with Test: Automated mechanisms implem AC-5(CMS-1) – Enhancement (High) Control Ensure that audit functions are not pe Applicability: All ASSESSMENT PROCEDURE: AC-5(Assessment Methods And Objects Examine: Separation of duties policy records; other relevant documents or enforces separation of duties through Interview: Organizational personnel with personnel with a constrained and a personnel with a constrained a personnel with a cons	eparation of duties through assigned access authorizations. redures addressing separation of duties; information system configuration settings and associated documentation; let relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy. erformed by security personnel responsible for administering access control. References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5 (CMS-1).1 hes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the re and procedures; information system configuration settings and associated documentation; list of separation of dutie records to determine if audit functions are NOT performed by security personnel responsible for administering access assigned access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit authorizations complement and reinforce separation of duties.	list of separation of duties authorizations; Related Controls: sponsibilities and duties of individuals. ies authorizations; information system audit ess control. Also, ensure that the organization
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; proci- information system audit records; other Interview: Organizational personnel with Test: Automated mechanisms implem AC-5(CMS-1) – Enhancement (High) Control Ensure that audit functions are not pe Applicability: All ASSESSMENT PROCEDURE: AC-5(Assessment Methods And Objects Examine: Separation of duties policy records; other relevant documents or enforces separation of duties through Interview: Organizational personnel with personnel. Also, determine if access Test: Automated mechanisms implem 	eparation of duties through assigned access authorizations. eedures addressing separation of duties; information system configuration settings and associated documentation; I er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy. erformed by security personnel responsible for administering access control. References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5 (CMS-1).1 hes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the re and procedures; information system configuration settings and associated documentation; list of separation of duti records to determine if audit functions are NOT performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are NOT performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are not performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit authorizations complement and reinforce separation of duties.	list of separation of duties authorizations; Related Controls: sponsibilities and duties of individuals. ies authorizations; information system audit ess control. Also, ensure that the organization
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; proci- information system audit records; other Interview: Organizational personnel with Test: Automated mechanisms implem AC-5(CMS-1) – Enhancement (High) Control Ensure that audit functions are not pe Applicability: All ASSESSMENT PROCEDURE: AC-5(Assessment Methods And Objects Examine: Separation of duties policy records; other relevant documents or enforces separation of duties through Interview: Organizational personnel with personnel. Also, determine if access Test: Automated mechanisms implem 	eparation of duties through assigned access authorizations. eedures addressing separation of duties; information system configuration settings and associated documentation; I er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy. erformed by security personnel responsible for administering access control. References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5 (CMS-1).1 hes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the re and procedures; information system configuration settings and associated documentation; list of separation of duti records to determine if audit functions are NOT performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are NOT performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are not performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit authorizations complement and reinforce separation of duties.	list of separation of duties authorizations; Related Controls: sponsibilities and duties of individuals. ies authorizations; information system audit ess control. Also, ensure that the organization
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; proci- information system audit records; other Interview: Organizational personnel with Test: Automated mechanisms implem AC-5(CMS-1) – Enhancement (High) Control Ensure that audit functions are not pe Applicability: All ASSESSMENT PROCEDURE: AC-5(Assessment Methods And Objects Examine: Separation of duties policy records; other relevant documents or enforces separation of duties through Interview: Organizational personnel with personnel. Also, determine if access Test: Automated mechanisms implem AC-5(CMS-2) – Enhancement (High) Control 	eparation of duties through assigned access authorizations. edures addressing separation of duties; information system configuration settings and associated documentation; lear relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy. erformed by security personnel responsible for administering access control. References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5 (CMS-1).1 hes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the re and procedures; information system configuration settings and associated documentation; list of separation of duti records to determine if audit functions are NOT performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit authorizations complement and reinforce separation of duties.	list of separation of duties authorizations; Related Controls: sponsibilities and duties of individuals. ies authorizations; information system audit ess control. Also, ensure that the organization
 (i) the organization establishes approp (ii) the information system enforces se Assessment Methods And Objects Examine: Access control policy; proci- information system audit records; other Interview: Organizational personnel with Test: Automated mechanisms implem AC-5(CMS-1) – Enhancement (High) Control Ensure that audit functions are not pe Applicability: All ASSESSMENT PROCEDURE: AC-5(Assessment Methods And Objects Examine: Separation of duties policy records; other relevant documents or enforces separation of duties through Interview: Organizational personnel with personnel. Also, determine if access Test: Automated mechanisms implem AC-5(CMS-2) – Enhancement (High) 	eparation of duties through assigned access authorizations. eedures addressing separation of duties; information system configuration settings and associated documentation; I er relevant documents or records. with responsibilities for defining appropriate divisions of responsibility and separation of duties. nenting separation of duties policy. erformed by security personnel responsible for administering access control. References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5 (CMS-1).1 hes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the re and procedures; information system configuration settings and associated documentation; list of separation of duti records to determine if audit functions are NOT performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are NOT performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit functions are not performed by security personnel responsible for administering access authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit authorizations. with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit authorizations complement and reinforce separation of duties.	list of separation of duties authorizations; Related Controls: sponsibilities and duties of individuals. ies authorizations; information system audit ess control. Also, ensure that the organization

ASSESSMENT PROCEDURE: AC-5(CMS-2).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. **Assessment Methods And Objects**

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization maintains a limited group of administrators with access based upon the users' roles and responsibilities. Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the number of personnel with root access is limited to only those personnel with a business need for root access.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-3) – Enhancement (High)

Control

Ensure that critical mission functions and information system support functions are divided among separate individuals.

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals. Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-4) – Enhancement (High)

Control

Ensure that information system testing functions (i.e., user acceptance, guality assurance, information security) and production functions are divided among separate individuals or groups,

Applicability: All	References: ARS: AC-5(CMS-4); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-5(CMS-4).1		

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records: other relevant documents or records to determine if information system testing functions (i.e., user acceptance, guality assurance, information security) and production functions are divided among separate individuals or groups.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-5) – Enhancement (High)

Control

Ensure that an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.

Applicability: All; Optional for SS	References: ARS: AC-5(CMS-5); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-5(CMS-5).1		

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the

information system, conducts information security testing of the information system. Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties. None of these individuals or functions should be conducting information security testing of the information system. Test: Automated mechanisms implementing separation of duties policy. AC-5(CMS-6) – Enhancement (High) Control Ensure that quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions are conducted by an independent entity, not the code developers. References: ARS: AC-5(CMS-6); FISCAM: TSD-1.1.2 **Related Controls:** Applicability: All ASSESSMENT PROCEDURE: AC-5(CMS-6).1 **Assessment Objective** Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. **Assessment Methods And Objects** Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions are conducted by an independent entity, not the code developers. Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if coders do their own quality assurance or code reviews. Test: Automated mechanisms implementing separation of duties policy. AC-5(FIS-1) – Enhancement (High) Control Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization. Applicability: All References: FISCAM: TSD-1.3.2 **Related Controls:** ASSESSMENT PROCEDURE: AC-5(FIS-1).1 Assessment Objective Determine if the organization provides adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization. Assessment Methods And Objects Examine: Pertinent policies and procedures. Interview: Personnel to determine whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties. AC-6 – Least Privilege (High) Control Each user or process shall be assigned the most restrictive set of privileges needed for the performance of authorized tasks. Guidance The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals. Applicability: All References: ARS: AC-6: FISCAM: TSD-2.1: HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A): HSPD 7: **Related Controls:** D(10): IRS-1075: 5.6.2.3#1. 5.6.3.2#3.2: NIST 800-53/53A: AC-6: PISP: 4.1.6 ASSESSMENT PROCEDURE: AC-6.1 **Assessment Objective** Determine if: (i) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks; and (ii) the information system enforces the most restrictive set of rights/privileges or accesses needed by users. **Assessment Methods And Objects** Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.

AC-6(CMS-1) – Enhancement (High)	
Control	
Disable all file system access not explicitly required for system, application, and administrator functionality.	
Applicability: All References: ARS: AC-6(CMS-1); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-6(CMS-1).1	
Assessment Objective	
Determine if the information system enforces separation of duties through assigned access authorizations.	
Assessment Methods And Objects	
Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information documentation; information system audit records; other relevant documents or records to determine if all file system access not explicitly refunctionality is disabled.	
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine determine if file system access not explicitly required for system, application, and administrator functionality are disabled.	hosts that store, transmit or process sensitive data to
Test: Information system hosts that store, transmit or process sensitive data to ensure that all file system access not explicitly required for	system, application, and administrator functionality is
disabled.	
AC-6(CMS-2) – Enhancement (High)	
Control	
Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. T contractor's ability to adhere to and support CMS security policy.	The contractor selection process must assess the
Applicability: All; Optional for SS References: ARS: AC-6(CMS-2); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-6(CMS-2).1	
Determine if the information system enforces separation of duties through assigned access authorizations. Assessment Methods And Objects Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information documentation; information system audit records; other relevant documents or records to determine if contractors are required to be provid they've agreed to support the CMS security requirements. The documented contractor selection process must assess the contractor's abili Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine all file system access not explicitly required for system, application, and administrator functionality is disabled.	led with minimal system and physical access, and that ty to adhere to and support CMS security policy.
Test: Information system hosts that store, transmit or process sensitive data; and that contain account information for contractors, to deter system, application, and administrator functionality is disabled.	mine if all file system access not explicitly required for
AC-6(CMS-3) – Enhancement (High)	
Control Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database dat Implement column-level access controls.	
Applicability: All References: ARS: AC-6(CMS-3); FISCAM: TAC-3.2.D.1, TAC-3.2.D.2, TAC-3.2.D.3, TA	C-3.2.D.4 Related Controls:
ASSESSMENT PROCEDURE: AC-6(CMS-3).1	
Assessment Objective	
Determine if the information system enforces separation of duties through assigned access authorizations.	
ssessment Methods And Objects	
Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information documentation; information system audit records; other relevant documents or records to determine if the information system restricts the u database administrators. Policies and procedures must also prevent users from accessing database data files at the logical data view, field controls.	use of database management utilities to only authorized
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine management utilities to only authorized database administrators. Also, determine whether or not users are prevented from accessing data levels. Column-level access controls must also be implemented.	base data files at the logical data view, field, or field-valu
Test: Information system hosting databases to determine if the information system restricts the use of database management utilities to or	nly authorized database administrators. Also, determine

Control	High)						
		there files					an isan that any summary human includes the
performance of job duties.	rs are permitted to	access those files,	directories, drives	, workstations, servers	, network snares, por	rts, protocols, and se	ervices that are expressly required for the
Applicability: All		References: ARS: 075: 5.1#1.1, 5.2#	(//	CAM: TAN-2.2.1; HIP/	A: 164.312(c)(1); HS	SPD 7: D(10); IRS-	Related Controls:
ASSESSMENT PROCEDURE: A			·, ·····				
Assessment Objective							
Determine if the information sys	tem enforces sena	ration of duties thro	undh assigned acco	ess authorizations			
Assessment Methods And Obj			agir accigned acci				
documentation; information syst servers, network shares, ports, p Interview: Organizational perso Ensure that only access to those assigned.	em audit records; of protocols, and serv onnel with responsil e files, directories, of a sample of user a	other relevant docu ices that are expre pilities for defining I drives, workstation	ments or records t ssly required for th east privileges nec s, servers, network	o determine if only aut e performance of job o cessary to accomplish a shares, ports, protoco	horized users are per duties. specified tasks to det ols, and services that	rmitted to access the ermine if the default are expressly requir	figuration settings and associated ose files, directories, drives, workstations t level of access for the various user type red for the performance of job duties are rk shares, ports, protocols, or services tha
AC-7 – Unsuccessful Log-o		liah)					
Control		··9··/					
Automated mechanisms shall be	e in place and supp cified time period.	oorting procedures Systems shall be lo	shall be developed ocked after a speci	l, documented, and im	plemented effectively e unsuccessful log-on	to enforce a limit of attempts.	f CMS-defined consecutive invalid access
Automated mechanisms shall be attempts by a user during a spec	e in place and supp cified time period.	oorting procedures Systems shall be le	shall be developed ocked after a speci	l, documented, and im fied number of multiple	plemented effectively e unsuccessful log-on	r to enforce a limit of a attempts.	f CMS-defined consecutive invalid access
Automated mechanisms shall be attempts by a user during a spece Guidance	cified time period.	Systems shall be le	ocked after a speci	fied number of multiple	e unsuccessful log-on	attempts.	f CMS-defined consecutive invalid access predetermined time period established b
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All	cified time period. f service, automatic	Systems shall be lockouts initiated l	ocked after a speci	fied number of multiple	e unsuccessful log-or	attempts. cally release after a	
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All	cified time period. f service, automatic	Systems shall be lockouts initiated l	ocked after a speci	fied number of multiple system are usually ten	e unsuccessful log-or	attempts. cally release after a	predetermined time period established b
Automated mechanisms shall be attempts by a user during a spece Guidance Due to the potential for denial of	cified time period. f service, automatic	Systems shall be lockouts initiated l	ocked after a speci	fied number of multiple system are usually ten	e unsuccessful log-or	attempts. cally release after a	predetermined time period established b
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if:	cified time period. f service, automatic R AC-7.1	Systems shall be k clockouts initiated l ceferences: ARS: A	ocked after a speci by the information AC-7; IRS-1075: 5.	fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5	e unsuccessful log-or nporary and automatio 33/53A: AC-7; PISP: 4	n attempts. cally release after a 4.1.7	predetermined time period established b Related Controls:
Automated mechanisms shall be attempts by a user during a spece Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the m	cified time period. f service, automatic R AC-7.1	Systems shall be k clockouts initiated l ceferences: ARS: A	ocked after a speci by the information AC-7; IRS-1075: 5.	fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5	e unsuccessful log-or nporary and automatio 33/53A: AC-7; PISP: 4	n attempts. cally release after a 4.1.7	predetermined time period established b
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enform	cified time period. f service, automatic R AC-7.1 naximum number concess the organizatio	Systems shall be k clockouts initiated l ceferences: ARS: A of consecutive inval n-defined limit of c	booked after a speci by the information AC-7; IRS-1075: 5 id access attempts onsecutive invalid	fied number of multiple system are usually ten .6.3.2#4.1; NIST 800-5 s to the information sys	e unsuccessful log-or nporary and automatio 33/53A: AC-7; PISP: 4 stem by a user and th	n attempts. cally release after a 4.1.7 e time period in whi	predetermined time period established b Related Controls:
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enform (iii) the organization defines the	cified time period. f service, automatic AC-7.1 naximum number construction ces the organization time period for lock er a lock out mode	Systems shall be k clockouts initiated l ceferences: ARS: A of consecutive inval n-defined limit of c c out mode or delay	bocked after a speci by the information a AC-7; IRS-1075: 5 id access attempts onsecutive invalid period;	fied number of multiple system are usually ten .6.3.2#4.1; NIST 800-5 s to the information syst access attempts by a t	e unsuccessful log-on aporary and automatic 33/53A: AC-7; PISP: 4 stem by a user and th user during the organi	n attempts. cally release after a 4.1.7 e time period in whi ization-defined time	predetermined time period established b Related Controls:
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enform (iii) the organization defines the (iv) the organization selects eith	cified time period. f service, automatic R AC-7.1 maximum number of ces the organizatio time period for lock er a lock out mode npts; and	Systems shall be k clockouts initiated l ceferences: ARS: A of consecutive inval n-defined limit of c c out mode or delay for the organizatio	bocked after a speci by the information a AC-7; IRS-1075: 5 id access attempts onsecutive invalid period; n-defined time peri	fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5 s to the information sys access attempts by a u od or delays next login	e unsuccessful log-on aporary and automatic 33/53A: AC-7; PISP: 4 stem by a user and th user during the organi	n attempts. cally release after a 4.1.7 e time period in whi ization-defined time	predetermined time period established b Related Controls: ich the consecutive invalid access attemp
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enform (iii) the organization defines the (iv) the organization selects eith consecutive invalid access attem (v) the information system enform	cified time period. f service, automatic f service, automatic R AC-7.1 naximum number of ces the organizatio time period for lock er a lock out mode npts; and ces the organizatio	Systems shall be k clockouts initiated l ceferences: ARS: A of consecutive inval n-defined limit of c c out mode or delay for the organizatio	bocked after a speci by the information a AC-7; IRS-1075: 5 id access attempts onsecutive invalid period; n-defined time peri	fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5 s to the information sys access attempts by a u od or delays next login	e unsuccessful log-on aporary and automatic 33/53A: AC-7; PISP: 4 stem by a user and th user during the organi	n attempts. cally release after a 4.1.7 e time period in whi ization-defined time	predetermined time period established b Related Controls: ich the consecutive invalid access attemp
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enform (iii) the organization defines the (iv) the organization defines the (iv) the organization selects eith consecutive invalid access attem (v) the information system enfor Assessment Methods And Obj Examine: Access control policy information system audit records	cified time period. f service, automatic f service, automatic R AC-7.1 maximum number of ces the organizatio time period for lock er a lock out mode npts; and ces the organizatio ects ; procedures addre s; other relevant do	Systems shall be k clockouts initiated l cleferences: ARS: A of consecutive inval n-defined limit of c c out mode or delay for the organizatio in-selected lock out ssing unsuccessfu	bocked after a speci by the information a AC-7; IRS-1075: 5. id access attempts onsecutive invalid a period; n-defined time period; mode or delayed I logon attempts; ir s.	fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5 s to the information syst access attempts by a to od or delays next login login prompt.	e unsuccessful log-or aporary and automatic 33/53A: AC-7; PISP: 4 stem by a user and th user during the organi a prompt for the organ	attempts. cally release after a 4.1.7 e time period in whi ization-defined time hization-defined dela	predetermined time period established b Related Controls: ich the consecutive invalid access attemp
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enfor (iii) the organization defines the (iv) the organization defines the (iv) the organization selects eith consecutive invalid access attern (v) the information system enfor Assessment Methods And Obj Examine: Access control policy information system audit records Test: Automated mechanisms in	cified time period. f service, automatic f service, automatic R AC-7.1 maximum number of ces the organizatio time period for lock er a lock out mode npts; and ces the organizatio ects ; procedures addre s; other relevant do	Systems shall be k clockouts initiated l cleferences: ARS: A of consecutive inval n-defined limit of c c out mode or delay for the organizatio in-selected lock out ssing unsuccessfu	bocked after a speci by the information a AC-7; IRS-1075: 5. id access attempts onsecutive invalid a period; n-defined time period; mode or delayed I logon attempts; ir s.	fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5 s to the information syst access attempts by a to od or delays next login login prompt.	e unsuccessful log-or aporary and automatic 33/53A: AC-7; PISP: 4 stem by a user and th user during the organi a prompt for the organ	attempts. cally release after a 4.1.7 e time period in whi ization-defined time hization-defined dela	predetermined time period established b Related Controls: ich the consecutive invalid access attemp period; ay period for information system response
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enform (iii) the organization defines the (iv) the organization defines the (iv) the organization selects eith consecutive invalid access attem (v) the information system enfor Assessment Methods And Obj Examine: Access control policy information system audit records	cified time period. f service, automatic f service, automatic R AC-7.1 maximum number of ces the organizatio time period for lock er a lock out mode npts; and ces the organizatio ects ; procedures addre s; other relevant do	Systems shall be k clockouts initiated l cleferences: ARS: A of consecutive inval n-defined limit of c c out mode or delay for the organizatio in-selected lock out ssing unsuccessfu	bocked after a speci by the information a AC-7; IRS-1075: 5. id access attempts onsecutive invalid a period; n-defined time period; mode or delayed I logon attempts; ir s.	fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5 s to the information syst access attempts by a to od or delays next login login prompt.	e unsuccessful log-or aporary and automatic 33/53A: AC-7; PISP: 4 stem by a user and th user during the organi a prompt for the organ	attempts. cally release after a 4.1.7 e time period in whi ization-defined time hization-defined dela	predetermined time period established b Related Controls: ich the consecutive invalid access attemp period; ay period for information system response
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enfor (iii) the organization defines the (iv) the organization defines the (iv) the organization selects eith consecutive invalid access attern (v) the information system enfor Assessment Methods And Obj Examine: Access control policy information system audit records Test: Automated mechanisms in AC-7(0) – Enhancement (High)	cified time period. f service, automatic f service, automatic R AC-7.1 maximum number of ces the organizatio time period for lock er a lock out mode npts; and ces the organizatio ects ; procedures addre s; other relevant do	Systems shall be k clockouts initiated l cleferences: ARS: A of consecutive inval n-defined limit of c c out mode or delay for the organizatio in-selected lock out ssing unsuccessfu	bocked after a speci by the information a AC-7; IRS-1075: 5. id access attempts onsecutive invalid a period; n-defined time period; mode or delayed I logon attempts; ir s.	fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5 s to the information syst access attempts by a to od or delays next login login prompt.	e unsuccessful log-or aporary and automatic 33/53A: AC-7; PISP: 4 stem by a user and th user during the organi a prompt for the organ	attempts. cally release after a 4.1.7 e time period in whi ization-defined time hization-defined dela	predetermined time period established b Related Controls: ich the consecutive invalid access attemp period; ay period for information system response
Automated mechanisms shall be attempts by a user during a spec Guidance Due to the potential for denial of organization. Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines the n occur; (ii) the information system enfor (iii) the organization defines the (iv) the organization defines the (iv) the organization selects eith consecutive invalid access attern (v) the information system enfor Assessment Methods And Obj Examine: Access control policy information system audit records Test: Automated mechanisms in AC-7(0) – Enhancement (High)	cified time period. f service, automatic f service, automatic R AC-7.1 naximum number of ces the organizatio time period for lock er a lock out mode npts; and ces the organizatio ects ; procedures addre s; other relevant do mplementing the act m to lock out the us	Systems shall be k clockouts initiated l cleferences: ARS: A of consecutive inval n-defined limit of c cout mode or delay for the organizatio in-selected lock out ssing unsuccessfu cours control policy er account automa	bocked after a speci by the information a AC-7; IRS-1075: 5. id access attempts onsecutive invalid a operiod; n-defined time period; mode or delayed I logon attempts; ir s. of or unsuccessful I tically after three (fied number of multiple system are usually ten 6.3.2#4.1; NIST 800-5 s to the information sys access attempts by a to od or delays next logir login prompt. nformation system sec ogin attempts.	ts by a user during a	attempts. cally release after a 4.1.7 e time period in whi ization-defined time nization-defined dela n system configuration one (1) hour time pro-	predetermined time period established b Related Controls: ich the consecutive invalid access attemp period; ay period for information system response

ASSESSMENT PROCEDURE: AC-7(0).1

Assessment Objective

Determine if the organization configures system lockout to assist in preventing password guessing.

Assessment Methods And Objects

Examine: Password lockout policy includes failed log-on attempts, lockout timeframes period for failed attempts and system/network administrator account reset capabilities. **Interview:** A sampling of users for knowledge of log-on and account lockout procedure policy is known.

Test: The account lockout function requires and administrator's reset of the locked-out user account.

AC-8 – System Use Notification (High)

Control

An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS information system.

Guidance

Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Applicability: All

References: ARS: AC-8; FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2; NIST 800-53/53A: AC-8; PISP: 4.1.8

ASSESSMENT PROCEDURE: AC-8.1

Assessment Objective

Determine if:

(i) the information system displays a system use notification message before granting system access informing potential users:

- that the user is accessing a U.S. Government information system;

- that system usage may be monitored, recorded, and subject to audit;

- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording;
- (ii) the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).
- (iii) the organization approves the information system use notification message before its use; and
- (iv) the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for system use notification.

AC-8(CMS-1) – Enhancement (High)

Control

Configure the information system to display a warning banner automatically prior to granting access to potential users. Notify users that:

(a) They are accessing a U.S. Government information system;

(b) CMS maintains ownership and responsibility for its computer systems;

(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;

(d) Their usage may be monitored, recorded, and audited;

(e) Unauthorized use is prohibited and subject to criminal and civil penalties; and

(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.

Guidance

All CMS information system computers and network devices under their control, independently, prominently and completely display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web, ftp, telnet, or other services accessed.

	Applicability: All	References: ARS: AC-8(CMS-1); FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.6.3.2#4.2	Related Controls:
--	--------------------	--	-------------------

Related Controls: SI-4

ASSESSMENT PROCEDURE: AC-8(CMS-1).1

Assessment Objective

- Determine if the information system displays a system use notification message before granting system access informing potential users:
- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- that use of the system indicates consent to monitoring and recording.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if the information system is configured to display a warning banner automatically prior to granting access to potential users. Notify users that: (a) They are accessing a U.S. Government information system;

- (b) CMS maintains ownership and responsibility for its computer systems;
- (c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
- (c) Users must adhere to CMS information Security Policies, Standards, and P
- (d) Their usage may be monitored, recorded, and audited;
- (e) Unauthorized use is prohibited and subject to criminal and civil penalties; and

(f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.

Interview: Organizational personnel to determine if hosts are configured to present a warning banner at system access points. The warning banner must contain the following elements:

- (a) They are accessing a U.S. Government information system;
- (b) CMS maintains ownership and responsibility for its computer systems;
- (c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;
- (d) Their usage may be monitored, recorded, and audited;
- (e) Unauthorized use is prohibited and subject to criminal and civil penalties; and
- (f) The use of the information system establishes their consent to any and all monitoring and recording of their activities.
- Test: Automated mechanisms implementing the access control policy for system use notification.

AC-8(CMS-2) – Enhancement (High)

Control

Develop and implement the warning banner in conjunction with legal counsel.

Applicability: All References: ARS: AC-8(CMS-2); IRS-1075: 5.6.3.2#4.2

ASSESSMENT PROCEDURE: AC-8(CMS-2).1

Assessment Objective

Determine if the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if warning banners were developed and implemented in conjunction with legal counsel.

Interview: Organizational personnel to determine if warning banners were developed and implemented in conjunction with legal counsel.

Test: Automated mechanisms implementing the access control policy for system use notification.

AC-8(CMS-3) – Enhancement (High)

Control

Post clear privacy policies on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.

Applicability: All	References: ARS: AC-8(CMS-3); IRS-1075: 5.6.3.2#4.2	Related Controls:		

ASSESSMENT PROCEDURE: AC-8(CMS-3).1

Assessment Objective

Determine if the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records to determine if clear privacy policies are posted on web sites, major entry points to a web site and any web page where substantial personal information from the public is collected.

Interview: Organizational personnel to determine if clear privacy policies are posted where substantial personal information from the public is collected.

Related Controls:

Test: Automated mechanisms implementing the	e access control policy for system use notification.	
AC-9 – Previous Log-on Notification (H	igh)	
Control		
Automated mechanisms shall be in place and s successful and unsuccessful.	upporting procedures shall be developed, documented, and implemented effectively to pr	rovide users with information about previous log-ons, both
Guidance		
provide an automated method of notifying the a	on may have the ability to log-on to a system or application using an authorized person's uthorized user of the last successful log-on date and time, and a number of previously un for authorized users to report unauthorized log-ons and unauthorized attempts to log-on.	log-on account, all systems and applicable applications will successful log-on attempts. It is important that training
Applicability: All	References: ARS: AC-9; NIST 800-53/53A: AC-9; PISP: 4.1.9	Related Controls: AC-7(0), CA-4(1), CA- 7(1)
ASSESSMENT PROCEDURE: AC-9.1		
Assessment Objective		
	essful logon, displays the date and time of the last logon and the number of unsuccessful	logon attempts since the last successful logon.
Assessment Methods And Objects		
	dressing previous logon notification; information system notification messages; informatic	on system design documentation; information system
	tation; other relevant documents or records.(Optional)	
	e access control policy for previous logon notification.(Optional)	
AC-9(0) – Enhancement (High)		
Control		
	ser, upon successful log-on, of the date and time of the last log-on, and the number of un	
	References: ARS: AC-9(0), 4.1.9	Related Controls:
ASSESSMENT PROCEDURE: AC-9(0).1		
Assessment Objective	mente co aposified in the baseline control and the aposifie CMC requirements on preservi	ad in this amplifying apparament to the baseline control
Assessment Methods And Objects	ments as specified in the baseline control and the specific CMS requirements as prescribe	ed in this amplifying enhancement to the baseline control.
	dressing previous logon notification; information system notification messages; informatic	on system design documentation: information system
configuration settings and associated document		Sh system design documentation, mormation system
	e access control policy for previous logon notification.	
AC-10 – Concurrent Session Control (H	ligh)	
Control		
Automated mechanisms shall be in place to lim information system.	t the number of concurrent user sessions, based upon the established business needs of	f the user, CMS, and the sensitivity level of the CMS
Guidance		
	ssions to function properly. However, based on the operational needs, automated mechar y system to have user concurrent sessions. Management should periodically review the r	
Applicability: All	References: ARS: AC-10; NIST 800-53/53A: AC-10; PISP: 4.1.10	Related Controls:
ASSESSMENT PROCEDURE: AC-10.1		
Assessment Objective		
Determine if:		
() S	er of concurrent sessions for information system users; and	
	concurrent sessions for users to the organization-defined number of sessions.	
Assessment Methods And Objects	dracsing concurrent session control: information system configuration actings and coord	viated documentation; information system costributation; other
relevant documents or records.	dressing concurrent session control; information system configuration settings and assoc	nated documentation, information system security plan; othe
	e access control policy for concurrent session control.	
,		

AC-10(0) – Enhancement (High)			
Control			
The number of concurrent User ID network log-on	sessions is limited and enforced to one (1) session. The number of concurrent a	application/process ses	ssions is limited and enforced to the number of
sessions expressly required for the performance of			
Applicability: All	References: ARS: AC-10(0); NIST 800-53/53A: AC-10; PISP: 4.1.10		Related Controls:
ASSESSMENT PROCEDURE: AC-10(0).1			
Assessment Objective			
Determine if the organization meets the requireme	ents as specified in the baseline control and the specific CMS requirements as pl	rescribed in this amplify	ying enhancement to the baseline control.
Assessment Methods And Objects			
Examine: Access control policy; procedures addre	essing concurrent session control; information system configuration settings and	associated document	ation; information system security plan (for
	for information system users); other relevant documents or records.		
1 2	access control policy for concurrent session control.		
AC-10(CMS-1) – Enhancement (High)			
Control			
The requirement and use of more than one (1) ap	plication/process session for each user is documented in the SSP.		
	References: ARS: AC-10(CMS-1)		Related Controls:
ASSESSMENT PROCEDURE: AC-10(CMS-1).1			
Assessment Objective			
Determine if the information system limits the num	nber of concurrent sessions for users to the organization-defined number of sess	sions.	
Assessment Methods And Objects	-		
Examine: Access control policy; procedures addre	essing concurrent session control; information system configuration settings and	associated document	ation; information system security plan (for
	for information system users); other relevant documents or records to determine	e if the requirement and	use of more than one (1) User ID network
log-on session for each user is documented in the			
-	if the information system allows more than one log-on session.		
	access control policy for concurrent session control.		
AC-11 – Session Lock (High)			
Control			
	lace and supporting procedures shall be developed, documented, and implement		
	tect inactivity and block further access until the user re-establishes the connection	on using proper identifi	cation and authentication processes.
Guidance			
	ns. A session lock is not a substitute for logging out of the information system. Of		
	norandum 06-16, the organization-defined time period is no greater than thirty mi		
	References: ARS: AC-11; IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-11; PIS	SP: 4.1.11	Related Controls:
ASSESSMENT PROCEDURE: AC-11.1			
Assessment Objective			
Determine if:			
() S	inactivity that initiates a session lock within the information system;		
	after the organization-defined time period of inactivity; and		
	lock until the user reestablishes access using appropriate identification and auth	entication procedures.	
Assessment Methods And Objects		r	
	essing session lock; information system design documentation; information system	em configuration settin	gs and associated documentation; information
system security plan; other relevant documents or Test: Automated mechanisms implementing the a			
AC-11(0) – Enhancement (High)			
Control		hantiaatan Managaraa	t) to most and local access
Configure systems to disable local access automa	atically after fifteen (15) minutes of inactivity. Require a password (see IA-5, Aut	nenticator Managemer	II) TO RESTORE IOCAL ACCESS.

Applicability: All	References: ARS: AC-11(0); FISCAM: TAC-3.2.C.3; IRS-1075: 5.6.3.2#4.3, 5.7.3#1; NIST 800-	Related Controls: IA-5
	53/53A: AC-11; PISP: 4.1.11	
ASSESSMENT PROCEDURE: AC-11(0).1		
Assessment Objective		
5	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ing enhancement to the baseline control.
Assessment Methods And Objects		
Examine: Access control policy; procedures add	Iressing session lock; information system design documentation; information system configuration setting	s and associated documentation; information
Test: Automated mechanisms implementing the	ne period for user inactivity after which automatic session lock is to be activated); other relevant documer	its or records.
AC-12 – Session Termination (High)		
Control		
	ate all inactive remote sessions (both user and information system sessions) automatically.	
Guidance	izational information system is appared by a user (or an information system) communicating through an	outernal non ergenization controlled
network (e.g., the Internet).	izational information system is accessed by a user (or an information system) communicating through an	external, non-organization-controlled
Applicability: All	References: ARS: AC-12; FISCAM: TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3;	Related Controls:
	NIST 800-53/53A: AC-12; PISP: 4.1.12	
ASSESSMENT PROCEDURE: AC-12.1		
Assessment Objective		
Determine if:		
	er inactivity that initiates a remote session termination within the information system; and	
	es a remote session after the organization-defined time period of inactivity.	
Assessment Methods And Objects		
	Iressing session termination; information system design documentation; information system configuration	settings and associated documentation;
information system security plan; other relevant of Test: Automated mechanisms implementing the		
AC-12(0) – Enhancement (High)		
Control		
	y terminate all remote sessions (user and information system) after 30 minutes of inactivity.	
Applicability: All	References: ARS: AC-12(0); FISCAM: TAC-3.2.C.3, TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075:	Related Controls:
	5.6.3.2#4.3; NIST 800-53/53A: AC-12; PISP: 4.1.12	
ASSESSMENT PROCEDURE: AC-12(0).1		
Assessment Objective		
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.		
Assessment Methods And Objects		
	Iressing session termination; information system design documentation; information system configuration	
	n-defined time period for user inactivity after which automatic session termination is to be activated); other	r relevant documents or records.
Test: Automated mechanisms implementing the	access control policy for session termination.	
AC-12(1) – Enhancement (High)		
Control		
Automatic session termination applies to local ar		
Applicability: All	References: ARS: AC-12(1); FISCAM: TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-12(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-12(1).1	NIST 000-05/00A. AC-12(1)	
ASSESSMENT PROCEDURE. AC-12(1).1 Assessment Objective		
Determine if automatic session termination appli	as to local and remote sessions	
	בי נט וטלמו מווע ובוווטנב אבאאווא.	

Assessment Methods And Objects

Examine: Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for session termination.

AC-13 – Supervision and Review—Access Control (High)

Control

Personnel shall be supervised and reviewed with respect to the usage of CMS information system access controls. Automated mechanisms shall be in place to facilitate the review of audit records, and any unusual activities shall be investigated in a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of users with significant information system roles and responsibilities shall be reviewed more frequently.

Guidance

The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST SP 800-92 provides guidance on computer security log management.

	:
2.1.3; HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: AC-13; PISP: 4.1.13	

ASSESSMENT PROCEDURE: AC-13.1

Assessment Objective

Determine if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records.

Interview: Organizational personnel with supervisory and access control responsibilities.

AC-13(1) – Enhancement (High)

Control

Employ automated mechanisms to facilitate the review of user activities.

Applicability: All	References: ARS: AC-13(1); NIST 800-53/53A: AC-13(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-13(1).1		

Accessment Objective

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.

AC-13(CMS-1) – Enhancement (High)

Control

Review integrity of files and directories for unexpected and/or unauthorized changes at least once per day. Automate the review of file creation, changes and deletions; and monitor permission changes. Generate alert notification for technical staff review and assessment.

Applicability: All	References: ARS: AC-13(CMS-1); FISCAM: TAC-2.1.5; HIPAA: 164.312(c)(2), 164.312(e)(2)(i)	Related Controls:

ASSESSMENT PROCEDURE: AC-13(CMS-1).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records to determine if files and directories are reviewed for unexpected and/or unauthorized changes at least once per day. The review of file creation, changes and deletions, and permission changes must be monitored automatically. Alert notifications must be generated for technical staff review and assessment.

Interview: Organizational personnel with supervisory and access control responsibilities to determine if the interview of files and directories	s for unexpected and/or unauthorized changes at least and
Interview: Organizational personnel with supervisory and access control responsibilities to determine if the integrity of files and directorie per day. Determine if file creation, changes and deletions, and permission changes are being reviewed automatically. Determine if alert	
being generated.	
Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.	
AC-13(CMS-2) – Enhancement (High)	
Control	
Enable logging of administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator	or privilages, system shutdowns, repeats, arrors and access
authorizations.	or privileges, system sinutuowits, reboots, errors and access
Applicability: All References: ARS: AC-13(CMS-2); FISCAM: TAC-2.1.5, TAN-2.1.8, TSS-2.1.3	Related Controls:
ASSESSMENT PROCEDURE: AC-13(CMS-2).1	
Assessment Objective	
Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user a	octivities
Assessment Methods And Objects	
Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational	I records of supervisory notices of disciplinary actions to
users; information system exception reports; other relevant documents or records to determine if logging of administrator and user accou	
authorizations is enabled.	
Interview: Organizational personnel with supervisory and access control responsibilities to determine if logging of administrator and user	account activities, system shutdowns, reboots, errors and
access authorizations is enabled.	
Test: Automated mechanisms supporting the access control policy for supervision and review of user activities.	
AC-13(CMS-3) – Enhancement (High)	
Control	
Inspect administrator groups, root accounts and other system related accounts on demand but at least once every seven (7) days to ensu	ure that unauthorized accounts have not been created.
Applicability: All References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.	
ASSESSMENT PROCEDURE: AC-13(CMS-3).1	
Assessment Objective	
Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user a	ctivities.
Assessment Methods And Objects	
Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information sy	stem design documentation: information system
configuration settings and associated documentation; other relevant documents or records to determine if administrator groups, root acc	
demand, but at least once every seven (7) days to ensure that unauthorized accounts have not been created.	
Interview: Organizational personnel with supervisory and access control responsibilities to determine if administrator groups, root accour	nts and other system related accounts are inspected on
demand, but at least once every seven (7) days to ensure that unauthorized accounts have not been created.	
Test: Automated mechanisms supporting the access control policy for supervision and review of user.	
AC-13(FIS-1) – Enhancement (High)	
Control	
Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions perform	ned.
Applicability: All References: FISCAM: TSD-1.1.4	Related Controls:
ASSESSMENT PROCEDURE: AC-13(FIS-1).1	
Assessment Objective	
Determine if the organizational supervisory personnel review transactions performed.	
Assessment Methods And Objects	
Examine: Activities and test transaction reviews.	
Examine: Pertinent policies and procedures.	
Interview: Management.	
AC-14 – Permitted Actions without Identification or Authentication (High)	
Control	
Based upon mission / business requirements, public access to CMS information systems without identification and authorization shall be	limited to public websites and other publicly available
Dere 20 - £ 207	DDCCM Amondiy A Attachment

authentication.		
Guidance	uiste en stille estille en en en en state stille sterne fer en elle instead en este en en elle treba en estille	tion custome (e.g., individuale concession of a lovel
information system at http://www.firstgov.gov	vithout identification and authentication for public websites or other publicly available information	ition systems (e.g., individuals accessing a rederal
Applicability: All	References: ARS: AC-14; NIST 800-53/53A: AC-14; PISP: 4.1.14	Related Controls: IA-2
ASSESSMENT PROCEDURE: AC-14.1	References: ARO: AO 14, NICT 000 00/00A: AO 14, 1101 . 4.1.14	
Assessment Objective	acuments encotions that can be performed on the information system without iden	atilization or outbontigation
Assessment Methods And Objects	ocuments specific user actions that can be performed on the information system without iden	
-	addressing permitted actions without identification and authentication; information system co	onfiguration settings and associated documentation:
information system security plan; other releva		
	the access control policy for permitted actions without identification and authentication.	
AC-14(0) – Enhancement (High)		
Control		
	nat can be performed on the information system without identification or authentication.	
Applicability: All	References: ARS: AC-14(0); NIST 800-53/53A: AC-14; PISP: 4.1.14	Related Controls:
ASSESSMENT PROCEDURE: AC-14(0).1		
Assessment Objective		
	irements as specified in the baseline control and the specific CMS requirements as prescribe	ed in this amplifying enhancement to the baseline control.
Assessment Methods And Objects	irements as specified in the baseline control and the specific CMS requirements as prescribe	d in this amplifying enhancement to the baseline control.
Assessment Methods And Objects Examine: Access control policy; procedures	addressing permitted actions without identification and authentication; information system co	
Assessment Methods And Objects	addressing permitted actions without identification and authentication; information system co	
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing	addressing permitted actions without identification and authentication; information system co	
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva	addressing permitted actions without identification and authentication; information system co ant documents or records.	
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication.	onfiguration settings and associated documentation;
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not	addressing permitted actions without identification and authentication; information system co ant documents or records.	onfiguration settings and associated documentation;
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information.	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object	onfiguration settings and associated documentation;
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication.	onfiguration settings and associated documentation;
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other relevant Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object	onfiguration settings and associated documentation;
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other relevant Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1)	tives while preventing unauthorized access to sensitive Related Controls:
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other relevant Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object	tives while preventing unauthorized access to sensitive Related Controls:
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other relevant Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accompliant access to accompliant access and authentication only to the extent necessary to accompliant access access to accompliant access access to access to access to access the extent necessary to access the access access to be performed without identification and authentication only to the extent necessary to access to access to be performed without identification and authentication only to the extent necessary to access to access to be performed without identification and authentication only to the extent necessary to access to access to access to access the access access to access to access the access access to access the access access to access the access to access the access access to access the access to access to access to	tives while preventing unauthorized access to sensitive Related Controls: omplish mission objectives.
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accompliant actions without identification and authentication; information system co	tives while preventing unauthorized access to sensitive Related Controls: omplish mission objectives.
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other relevant Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures organization-defined actions that can be perfor	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accompliant actions without identification and authentication; information system co addressing permitted actions without identification; other relevant documents or records.	tives while preventing unauthorized access to sensitive Related Controls: omplish mission objectives.
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other relevant Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures organization-defined actions that can be perfor Interview: Organizational personnel with res	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accompliant actions without identification and authentication; information system co	tives while preventing unauthorized access to sensitive Related Controls: omplish mission objectives.
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures organization-defined actions that can be perfor Interview: Organizational personnel with res AC-15 – Automated Marking (High)	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accompliant actions without identification and authentication; information system co addressing permitted actions without identification; other relevant documents or records.	tives while preventing unauthorized access to sensitive Related Controls: omplish mission objectives.
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures organization-defined actions that can be perfor Interview: Organizational personnel with res AC-15 – Automated Marking (High) Control	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accomplish addressing permitted actions without identification and authentication; information system co ormed without identification and authentication; other relevant documents or records. ponsibilities for defining permitted actions without identification and authentication and authentication.	tives while preventing unauthorized access to sensitive Related Controls: omplish mission objectives. onfiguration settings and associated documentation; list of
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures organization-defined actions that can be perfor Interview: Organizational personnel with res AC-15 – Automated Marking (High) Control Automated mechanisms shall be in place to r	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accompliant actions without identification and authentication; information system co addressing permitted actions without identification; other relevant documents or records.	tives while preventing unauthorized access to sensitive Related Controls: omplish mission objectives. onfiguration settings and associated documentation; list of
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures organization-defined actions that can be perfor Interview: Organizational personnel with res AC-15 – Automated Marking (High) Control Automated mechanisms shall be in place to r instructions.	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accomplish addressing permitted actions without identification and authentication; information system co ormed without identification and authentication; other relevant documents or records. ponsibilities for defining permitted actions without identification and authentication and authentication.	tives while preventing unauthorized access to sensitive Related Controls: omplish mission objectives. onfiguration settings and associated documentation; list of
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures organization-defined actions that can be perfor Interview: Organizational personnel with res AC-15 – Automated Marking (High) Control Automated mechanisms shall be in place to r instructions. Guidance	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to acco addressing permitted actions without identification and authentication; information system co ormed without identification and authentication; other relevant documents or records. ponsibilities for defining permitted actions without identification and authentication and authentication.	any special dissemination, handling, or distribution
Assessment Methods And Objects Examine: Access control policy; procedures information system security plan; other releva Test: Automated mechanisms implementing AC-14(1) – Enhancement (High) Control Ensure that public users (users who have not information. Applicability: All ASSESSMENT PROCEDURE: AC-14(1).1 Assessment Objective Determine if the organization permits actions Assessment Methods And Objects Examine: Access control policy; procedures organization-defined actions that can be perfor Interview: Organizational personnel with res AC-15 – Automated Marking (High) Control Automated mechanisms shall be in place to r instructions. Guidance	addressing permitted actions without identification and authentication; information system co ant documents or records. the access control policy for permitted actions without identification and authentication. t been authenticated) only have access to the extent necessary to accomplish mission object References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1) to be performed without identification and authentication only to the extent necessary to accomplish addressing permitted actions without identification and authentication; information system co ormed without identification and authentication; other relevant documents or records. ponsibilities for defining permitted actions without identification and authentification and authentication.	any special dissemination, handling, or distribution

ASSESSMENT PROCEDURE: AC-15.1 Assessment Objective Determine if: (i) the organization identifies standard naming conventions for information system output: and (ii) the information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions. **Assessment Methods And Objects** Examine: Access control policy: procedures for addressing automated marking of information system output: information system output: information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Interview: Organizational personnel with responsibilities for defining special dissemination, handling, and marking instructions for information system output. Test: Automated mechanisms implementing automated marking of information system output. AC-16 – Automated Labeling (High) Control CMS information systems shall label information "in storage," "in process," and "in transit" with special dissemination handling or distribution instructions, in a manner consistent with this policy. Guidance Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy. References: ARS: AC-16: NIST 800-53/53A; AC-16: PISP: 4.1.16 Related Controls: AC-15 Applicability: All **ASSESSMENT PROCEDURE: AC-16.1 Assessment Objective** Determine if the information system appropriately labels information in storage, in process, and in transmission. Assessment Methods And Objects Examine: Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation: other relevant documents or records.(Optional) Test: Automated mechanisms implementing automated (internal) labeling within the information system.(Optional) AC-16(CMS-1) – Enhancement (High) Control If automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling). Applicability: All References: ARS: AC-16(CMS-1) **Related Controls:** ASSESSMENT PROCEDURE: AC-16(CMS-1).1 **Assessment Objective** Determine if the information system appropriately labels information in storage, in process, and in transmission. **Assessment Methods And Objects** Examine: Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine, if automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling). Interview: Organization personnel to determine, if automated information labeling is utilized, that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling). Test: Automated mechanisms implementing automated (internal) labeling within the information system. AC-17 – Remote Access (High) Control Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can access the information system from remote locations shall be limited and justification / approval for such access shall be controlled, documented, and monitored. Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, shall not be used to gain access to a CMS information system that processes CMS sensitive information unless the CIO or his/her designated representative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-

up capabilities.		
Guidance		
Internet). Examples of remote access methor specifically designed for public access. The c	tional information system by a user (or an information system) communicating through an external, non-orga ds include dial-up, broadband, and wireless. Remote access controls are applicable to information systems or organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon uthorized connections (e.g., using virtual private network technology). NIST SP 800-63 provides guidance or	other than public web servers or systems source of request) or protects against
federal Personal Identity Verification (PIV) cre	edential is used as an identification token where cryptographic token-based access control is employed, the 73 and 800-78. NIST SP 800-77 provides guidance on IPSec-based virtual private networks.	
Applicability: All	References: ARS: AC-17; FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800- 53/53A: AC-17; PISP: 4.1.17	Related Controls: IA-2, SC-9
ASSESSMENT PROCEDURE: AC-17.1		
Assessment Objective		
Determine if the organization documents, mo	pnitors, and controls all methods of remote access to the information system.	
Assessment Methods And Objects		
Examine: Access control policy; procedures records; other relevant documents or records	addressing remote access to the information system; information system configuration settings and associa	ted documentation; information system audit
Interview: Organizational personnel with ren	note access authorization, monitoring, and control responsibilities.	
AC-17(1) – Enhancement (High)		
Control		
Employ automated mechanisms to facilitate t	the monitoring and control of remote access methods.	
Applicability: All	References: ARS: AC-17(1); IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-17(1).1		
Assessment Objective Determine if the information system employs	automated mechanisms to facilitate the monitoring and control of remote access methods.	
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing	addressing remote access to the information system; information system configuration settings and associa	ited documentation; other relevant document
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High)	addressing remote access to the information system; information system configuration settings and associa	ited documentation; other relevant document
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access.	ited documentation; other relevant document
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access.	
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access.	
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-	
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-	
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-	
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC- 17(2)	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC- 17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records.	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or Test: Automated mechanisms implementing	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC- 17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records.	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or Test: Automated mechanisms implementing AC-17(3) – Enhancement (High)	addressing remote access to the information system; information system configuration settings and associa the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC- 17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records.	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or Test: Automated mechanisms implementing AC-17(3) – Enhancement (High) Control	addressing remote access to the information system; information system configuration settings and associate the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records. cryptographic protections for remote access.	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or Test: Automated mechanisms implementing AC-17(3) – Enhancement (High) Control Control Control all remote access through a limited n	addressing remote access to the information system; information system configuration settings and associate the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records. cryptographic protections for remote access. number of managed access control points.	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or Test: Automated mechanisms implementing AC-17(3) – Enhancement (High) Control Control all remote access through a limited n Applicability: All	addressing remote access to the information system; information system configuration settings and associate the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records. cryptographic protections for remote access.	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or Test: Automated mechanisms implementing AC-17(3) – Enhancement (High) Control Control all remote access through a limited n Applicability: All ASSESSMENT PROCEDURE: AC-17(3).1	addressing remote access to the information system; information system configuration settings and associate the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records. cryptographic protections for remote access. number of managed access control points.	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or Test: Automated mechanisms implementing AC-17(3) – Enhancement (High) Control Control all remote access through a limited n Applicability: All ASSESSMENT PROCEDURE: AC-17(3).1 Assessment Objective	addressing remote access to the information system; information system configuration settings and associate the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records. cryptographic protections for remote access. number of managed access control points.	Related Controls:
Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures or records. Test: Automated mechanisms implementing AC-17(2) – Enhancement (High) Control Employ cryptography to protect the confident Applicability: All ASSESSMENT PROCEDURE: AC-17(2).1 Assessment Objective Determine if the information system employs Assessment Methods And Objects Examine: Access control policy; procedures documentation; other relevant documents or Test: Automated mechanisms implementing AC-17(3) – Enhancement (High) Control	addressing remote access to the information system; information system configuration settings and associate the access control policy for remote access. tiality and integrity of remote access sessions. References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17(2) cryptography to protect the confidentiality and integrity of remote access sessions. addressing remote access to the information system; information system design documentation; information records. cryptographic protections for remote access. number of managed access control points.	Related Controls:

	trol points for remote access to the information system; and cesses through a limited number of managed access control points.	
Assessment Methods And Objects		
	Iressing remote access to the information system; information system design documentation; list of man	aged access control points; information
	cumentation; information system audit records; other relevant documents or records.	
Test: Automated mechanisms implementing the	access control policy for remote access.	
.C-17(4) – Enhancement (High)		
ontrol		i na se se
	ly for compelling operational needs and document the rationale for such access in the security plan for the References: ARS: AC-17(4); FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5; NIST 800-53/53A:	
pplicability: All	AC-17(4)	Related Controls.
SSESSMENT PROCEDURE: AC-17(4).1		
ssessment Objective		
Determine if:		
(i) the organization defines the situations and co	mpelling operational needs when remote access to privileged functions on the information system is allo	wed; and
(ii) the organization permits remote access for p	ivileged functions only for compelling operational needs and documents the rationale for such access in	the security plan for the information system
ssessment Methods And Objects		
	Iressing remote access to the information system; information system configuration settings and associa	ted documentation; information system
security plan; information system audit records;		
Test: Automated mechanisms implementing the	access control policy for remote access.	
C-17(CMS-1) – Enhancement (High)		
ontrol		
	VPN link(s) if connected to the information system and using remote administration. Utilize an approver password authentication or additional authentication protection (e.g., token-based).	d encryption standard (see SC-13, Use of
pplicability: All	References: ARS: AC-17(CMS-1); IRS-1075: 5.6.3.2#5	Related Controls: SC-13
SSESSMENT PROCEDURE: AC-17(CMS-1)	1	
ssessment Objective		
-	rs, and controls all methods of remote access to the information system.	
ssessment Methods And Objects		
	Iressing remote access to the information system; list of information system accounts; information system	
	s; other relevant documents or records to determine if secure management protocols through a VPN link	
	n that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination	with password authentication or additional
authentication protection (e.g., token-based) is r	equired to access system.	a = b + b + a + b = b + b = b + b + b + b + b + b + b
	tion are enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP	
, ,	tion (e.g., token-based) is required to access system.	
•	access control policy for remote access to determine that an approved encryption standard (see SC-13,	Use of Cryptography, PISP 4.16.13) in
	litional authentication protection (e.g., token-based) is required to access system.	
C-17(CMS-2) – Enhan <u>cement (High)</u>		
	ss connections.	
ontrol Implement password protection for remote acce pplicability: All	References: ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5	Related Controls:
ontrol Implement password protection for remote acce pplicability: All	References: ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5	Related Controls:
ontrol Implement password protection for remote acce pplicability: All SSESSMENT PROCEDURE: AC-17(CMS-2)	References: ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5	Related Controls:
ontrol Implement password protection for remote acce pplicability: All SSESSMENT PROCEDURE: AC-17(CMS-2) ssessment Objective	References: ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5	Related Controls:
ontrol Implement password protection for remote acce pplicability: All SSESSMENT PROCEDURE: AC-17(CMS-2) ssessment Objective Determine if the organization documents, monitor	References: ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5 1	Related Controls:
pplicability: All SSESSMENT PROCEDURE: AC-17(CMS-2) ssessment Objective Determine if the organization documents, monito ssessment Methods And Objects	References: ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5 1	

documentation; information system audit records; other relevant documents or records to determine if password protection for remote access connections is implemented. Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if password protection is required for remote access connections. Test: Automated mechanisms implementing the access control policy for remote access to determine remote access connections by attempting to gain access without a password.

AC-17(CMS-3) – Enhancement (High)

Control

Require callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified every 365 days.

Applicability: All	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	Related Controls:
ASSESSMENT PROCEDURE: AC-17(CMS-3)	ASSESSMENT PROCEDURE: AC-17(CMS-3),1	

Assessment Objective

Determine if:

(i) the organization defines managed access control points for remote access to the information system; and

(ii) the information system controls all remote accesses through a limited number of managed access control points.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified annually.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually. **Test:** Automated mechanisms implementing the access control policy for remote access to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually.

AC-17(CMS-4) – Enhancement (High)

Control

If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix A for e-Authentication standards.

 Applicability: All
 References: ARS: AC-17(CMS-4); IRS-1075: 5.6.3.2#5
 Related Controls:

 ASSESSMENT PROCEDURE: AC-17(CMS-4).1
 Related Controls:
 Related Controls:

Assessment Objective

Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if e-authentication is implemented as a remote access solution or associated with remote access. If so, refer to ARS Appendix A for e-Authentication standards.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system implements e-authentication. If so, refer to ARS Appendix A for e-Authentication standards.

Test: Automated mechanisms implementing the access control policy for remote access to determine if e-authentication is implemented. If so, refer to ARS Appendix A for e-Authentication standards.

AC-17(FIS-1) – Enhancement (High)

Control

Remote access phone numbers are not published and are periodically changed.

Applicability: All References: FISCAM: TAC-3.2.E.2.2

2.E.2.2

Related Controls:

ASSESSMENT PROCEDURE: AC-17(FIS-1).1

Assessment Objective

Determine if the organization changes, periodically, remote access phone numbers and those phone numbers are not published.

Assessment Methods And Objects	
Examine: Documentation showing changes to dial-in numbers.	
Examine: Entity's telephone directory to verify that the numbers are not listed.	
Examine: Pertinent policies and procedures.	
Interview: Remote access users.	
AC-18 – Wireless Access Restrictions (High)	
Control	
Installation of wireless access points (WAP) into CMS information systems and networks shall be prohibited unless explicitly authoriz representative. Authorized WAP devices and wireless access shall be monitored on a regular basis, and wireless communications s	
Guidance	
NIST SP 800-48 and 800-97 provide guidance on wireless network security. NIST SP 800-94 provides guidance on wireless intrusio	
Applicability: All References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18	Related Controls:
ASSESSMENT PROCEDURE: AC-18.1	
Assessment Objective	
Determine if:	
(i) the organization establishes usage restrictions and implementation guidance for wireless technologies;	
(ii) the organization authorizes, monitors, and controls wireless access to the information system; and	
(iii) the wireless access restrictions are consistent with NIST SP 800-48 and 800-97.	
Assessment Methods And Objects	
Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 monitoring, and control; information system audit records; other relevant documents or records.	and 800-97; activities related to wireless authorization,
Test: Wireless access usage and restrictions.	
AC-18(0) – Enhancement (High)	
Control	
CMS policy prohibits the use of wireless access unless explicitly approved by the CMS CIO or his/her designated representative.	
Applicability: All References: ARS: AC-18(0); NIST 800-53/53A: AC-18; PISP: 4.1.18	Related Controls:
ASSESSMENT PROCEDURE: AC-18(0).1	
Assessment Objective	
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as pres	scribed in this amplifying enhancement to the baseline control.
Assessment Methods And Objects	
Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48	3 and 800-97; activities related to wireless authorization,
monitoring, and control; information system audit records; other relevant documents or records.	
Test: Wireless access usage and restrictions.	
AC-18(1) – Enhancement (High)	
Control	
If wireless access is explicitly approved, approved authentication and encryption is used to protect wireless access to the information	
Applicability: All References: ARS: AC-18(1); NIST 800-53/53A: AC-18(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-18(1).1	
Assessment Objective	
Determine if the organization uses authentication and encryption to protect wireless access to the information system.	
Assessment Methods And Objects	
Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system settings and associated documentation; information system audit records; other relevant documents or records.	em design documentation; information system configuration
Test: Automated mechanisms implementing the access control policy for wireless access to the information system.	

AC-18(2) – Enhancement (High)		
Control		
	ess access points and take appropriate action if any access points are discover	2d
Guidance		
	uthorized wireless access points in facilities containing high-impact information	systems. The scan is not limited to only those areas within the facility
containing the high-impact information systems		
Applicability: All	References: ARS: AC-18(2); NIST 800-53/53A: AC-18(2)	Related Controls:
ASSESSMENT PROCEDURE: AC-18(2).1		Related Controls.
Assessment Objective		
Determine if: (i) the ergenization defines the frequency of erg	ans for unauthorized wireless access points; and	
	eless access points in accordance with organization-defined frequency and take	a appropriate action if such an appropriate are discovered
	sess access points in accordance with organization-defined frequency and take	es appropriate action il such an access points are discovered.
Assessment Methods And Objects		
	ddressing wireless implementation and usage (including restrictions); wireless s	canning reports; other relevant documents or records.
Test: Scanning procedure for unauthorized wir	eless access points.	
AC-18(DIR-1) – Enhancement (High)		
Control		
	ss devices, service set identifier broadcasting is disabled and the following wire	ess access controls are implemented:
(a) encryption protection is enabled;		
(b) access points are placed in secure areas;		
(c) access points are shut down when not in us	e (i.e., nights, weekends);	
 (d) a firewall is implemented between the wirele (e) MAC address authentication is utilized; 	ess network and the whed initastructure,	
(f) static IP addresses, not DHCP, is utilized;		
(g) personal firewalls are utilized on all wireless	s clients:	
(h) file sharing is disabled on all wireless clients		
(i) Intrusion detection agents are deployed on the		
(j) wireless activity is monitored and recorded, a	and the records are reviewed on a regular basis.	
Applicability: All	References:	Related Controls:
ASSESSMENT PROCEDURE: AC-18(DIR-1).	.1	
Assessment Objective		
	ess policies and strict procedures that control access to the wireless LAN and se	eparates/restricts the wireless LAN from the wired network infrastructure
Assessment Methods And Objects		•
	nuous wireless intrusion monitoring of approved and operational wireless syster	ns.
	less LAN records know what to look for in the data for an unauthorized intrusion	
	vireless devices into the approved wireless network infrastructure.	
AC-19 – Access Control for Portable ar	ia mobile Devices (Fign)	
	id Mobile Devices (High)	
Control The connection of portable and mobile devices	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone	es, and other computing and communications devices with network
Control The connection of portable and mobile devices connectivity and the capability of periodically op	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone berating in different physical locations) to CMS information systems and networ	ks shall be prohibited unless explicitly authorized, in writing, by the CIC
Control The connection of portable and mobile devices connectivity and the capability of periodically op or his/her designated representative. Prior to c	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone perating in different physical locations) to CMS information systems and networ connecting portable and mobile devices to CMS information systems and netwo	ks shall be prohibited unless explicitly authorized, in writing, by the CIC rks, such devices shall be configured to comply with CMS IS policies
Control The connection of portable and mobile devices connectivity and the capability of periodically op or his/her designated representative. Prior to c and procedures. The storage and transmissior	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone perating in different physical locations) to CMS information systems and networ connecting portable and mobile devices to CMS information systems and netwo of CMS sensitive information on portable and mobile information devices shall	ks shall be prohibited unless explicitly authorized, in writing, by the CIC rks, such devices shall be configured to comply with CMS IS policies be protected with activities such as scanning the devices for malicious
Control The connection of portable and mobile devices connectivity and the capability of periodically op or his/her designated representative. Prior to c and procedures. The storage and transmissior code, virus protection software, and disabling u	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone perating in different physical locations) to CMS information systems and networ connecting portable and mobile devices to CMS information systems and netwo	ks shall be prohibited unless explicitly authorized, in writing, by the CIO rks, such devices shall be configured to comply with CMS IS policies be protected with activities such as scanning the devices for malicious
Control The connection of portable and mobile devices connectivity and the capability of periodically op or his/her designated representative. Prior to c and procedures. The storage and transmissior code, virus protection software, and disabling u Guidance	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone perating in different physical locations) to CMS information systems and networ connecting portable and mobile devices to CMS information systems and netwo of CMS sensitive information on portable and mobile information devices shall innecessary hardware. The activities and controls shall be commensurate with	ks shall be prohibited unless explicitly authorized, in writing, by the CIO rks, such devices shall be configured to comply with CMS IS policies be protected with activities such as scanning the devices for malicious the system security level of the information.
Control The connection of portable and mobile devices connectivity and the capability of periodically op or his/her designated representative. Prior to c and procedures. The storage and transmissior code, virus protection software, and disabling u Guidance Portable and mobile devices (e.g., notebook co	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone perating in different physical locations) to CMS information systems and networ connecting portable and mobile devices to CMS information systems and networ of CMS sensitive information on portable and mobile information devices shall innecessary hardware. The activities and controls shall be commensurate with omputers, personal digital assistants, cellular telephones, and other computing a	ks shall be prohibited unless explicitly authorized, in writing, by the CIO rks, such devices shall be configured to comply with CMS IS policies be protected with activities such as scanning the devices for malicious the system security level of the information.
Control The connection of portable and mobile devices connectivity and the capability of periodically op or his/her designated representative. Prior to c and procedures. The storage and transmissior code, virus protection software, and disabling u Guidance Portable and mobile devices (e.g., notebook co of periodically operating in different physical loc	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone perating in different physical locations) to CMS information systems and networ connecting portable and mobile devices to CMS information systems and networ of CMS sensitive information on portable and mobile information devices shall innecessary hardware. The activities and controls shall be commensurate with omputers, personal digital assistants, cellular telephones, and other computing a cations) are only allowed access to organizational information systems in accord	ks shall be prohibited unless explicitly authorized, in writing, by the CIO rks, such devices shall be configured to comply with CMS IS policies be protected with activities such as scanning the devices for malicious the system security level of the information. and communications devices with network connectivity and the capabilit dance with organizational security policies and procedures. Security
connectivity and the capability of periodically op or his/her designated representative. Prior to c and procedures. The storage and transmission code, virus protection software, and disabling u Guidance Portable and mobile devices (e.g., notebook co of periodically operating in different physical loc	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone perating in different physical locations) to CMS information systems and networ connecting portable and mobile devices to CMS information systems and networ of CMS sensitive information on portable and mobile information devices shall innecessary hardware. The activities and controls shall be commensurate with omputers, personal digital assistants, cellular telephones, and other computing a	ks shall be prohibited unless explicitly authorized, in writing, by the CIO rks, such devices shall be configured to comply with CMS IS policies be protected with activities such as scanning the devices for malicious the system security level of the information. and communications devices with network connectivity and the capabilit dance with organizational security policies and procedures. Security
Control The connection of portable and mobile devices connectivity and the capability of periodically op or his/her designated representative. Prior to c and procedures. The storage and transmissior code, virus protection software, and disabling u Guidance Portable and mobile devices (e.g., notebook co of periodically operating in different physical loc	(e.g., notebook computers, personal digital assistants (PDA), cellular telephone perating in different physical locations) to CMS information systems and networ connecting portable and mobile devices to CMS information systems and networ of CMS sensitive information on portable and mobile information devices shall innecessary hardware. The activities and controls shall be commensurate with omputers, personal digital assistants, cellular telephones, and other computing a cations) are only allowed access to organizational information systems in accord	ks shall be prohibited unless explicitly authorized, in writing, by the CIO rks, such devices shall be configured to comply with CMS IS policies be protected with activities such as scanning the devices for malicious the system security level of the information. and communications devices with network connectivity and the capabilit dance with organizational security policies and procedures. Security

scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family.

Applicability: All	References: ARS: AC-19; IRS-1075: 4.6#1; NIST 800-53/53A: AC-19; PISP: 4.1.19	Related Controls: MP-4, MP-5

ASSESSMENT PROCEDURE: AC-19.1

Assessment Objective

Determine if:

(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;

- (ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and
- (iii) the organization authorizes, monitors, and controls device access to organizational information systems.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel who use portable and mobile devices to access the information system.

Test: Automated mechanisms implementing access control policy for portable and mobile devices.

AC-19(CMS-1) – Enhancement (High)

Control

If portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative:

Employ an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Applicability: All	References: ARS: AC-19(CMS-1); FISCAM: TAC-3.3; IRS-1075: 4.6#1, 4.7.2#1	Related Controls: MA-CMS-1, MA-CMS-2, SC-13

ASSESSMENT PROCEDURE: AC-19(CMS-1).1

Assessment Objective

Determine if:

(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices;

(ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and

(iii) the organization authorizes, monitors, and controls device access to organizational information systems.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records to determine if portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative. Also, determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Interview: Organizational personnel who use portable and mobile devices to access the information system to determine if portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative. Also, determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Test: Automated mechanisms implementing access control policy for portable and mobile devices to determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

AC-20 – Use of External Information Systems (High)

Control

External information systems, including, but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports shall not be used to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative.

Strict terms and conditions shall be established for the use of external information systems. The terms and conditions shall address, at a minimum: 4.1.20.1. The types of applications that can be accessed from external information systems;

4.1.20.2. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;			
4.1.20.3. How other users of the external information system will be prevented from accessing federal information;			
4.1.20.4. The use of virtual private networking (VPN) and firewall technologies;			
4.1.20.5. The use of and protection against the vulnerabilities of wireless technologies;			
4.1.20.6. The maintenance of adequate physical security controls;			
4.1.20.7. The use of virus and spyware protection software; and			
4.1.20.8. How often the security capabilities of installed software are to be updated.			
Guidance			
External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information systems. This control does not apply to the use of external information systems). The organization establishes terms and conditions for the use of external information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and			
procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.	from the external mornation system, and (ii)		
	Related Controls:		
Applicability: All References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20 4.1.20	Related Controls:		
ASSESSMENT PROCEDURE: AC-20.1			
Assessment Objective			
Determine if			
(i) the organization defines the types of applications that can be accessed from the external information system;			
(ii) the organization defines the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external inform	nation system: and		
(iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that			
accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that			
on the external information system.			
Assessment Methods And Objects			
Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of	of types of applications accessible from		
external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; informat			
associated documentation; other relevant documents or records.	, , , , , , , , , , , , , , , , , , , ,		
Interview: Organizational personnel who use external information systems to access the information system.			
AC-20(1) – Enhancement (High)			
Control			
Users are prohibited from using any external information system to access the information system or to process, store, or transmit CMS-controlled information organization:	ation except in situations where the		
(a) Can verify the employment of required security controls on the external system as specified in CMS' information security policy and the organization's (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.	system security plan; or		
Applicability: All References: ARS: AC-20(1); IRS-1075: 4.7.2#1; NIST 800-53/53A: AC-20(1)	Related Controls:		
SSESSMENT PROCEDURE: AC-20(1).1			
Assessment Objective			
Determine if the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:			
allowing connections to the external information system; or	- verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization's information security policy and system security plan when		
- approves, for authorized exceptions, information system connection or processing agreements with the organizational entity hosting the external information system.			
Assessment Methods And Objects			
Examine: Access control policy; procedures addressing the use of external information systems; information system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records.			

AC-20(CMS-1) – Enhancement (High)

Control

Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.

Applicability: All	References: ARS: AC-20(CMS-1); IRS-1075: 4.7.2#1, 4.7.3#3	Related Controls:
ASSESSMENT PROCEDURE: AC-20(CMS-1)	1	

Assessment Objective

Determine if the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

Interview: Organizational personnel who use external information systems to access the information system to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

AC-20(PII-1) – Enhancement (High)

Control

Only organization owned computers and software can be used to process, access, and store PII.

Applicability: All	References: IRS-1075: 4.7.1#1

ASSESSMENT PROCEDURE: AC-20(PII-1).1

Assessment Objective

Determine if the organizational computers and software are owned by that organization that processes, accesses and stores PII.

Assessment Methods And Objects

Examine: Organizational computer and software purchase orders indicating ownership of computers and software used to process, access and store PII.

Interview: Organizational staff indicating that only organizational owned computers and software are used to process, access and store PII.

AC-CMS-1 – System Boot Access (High)

Control

System boot access shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can alter or perform non-standard boots of systems and/or components of the information system shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Guidance

When a person has unrestrained physical access to any computing system or network device the person has control of the equipment.

If the person does not have the capability to locally access the information system's data though the boot process this can assist in protecting the data from loss or unauthorized access to the data. Note: Even though the system root access may be protected by privilege access controls a miss configured system can allow the system to reboot and thus allowing a boot / access from unauthorized media. An example of this is a LINUX system, not configured correctly, when CONT+ALT+DEL is issued from the keyboard the equipment will re-boot automatically.

Applicability: All	References: ARS: AC-CMS-1; PISP: 4.1.21	Related Controls:
ASSESSMENT PROCEDURE: AC-CMS-1.1	-	

Assessment Objective

Determine if the organization assesses the need for system boot access and if necessary controls, documents and monitors the continued need for system boot access.

Assessment Methods And Objects

Examine: System boot access documentation to determine that there is or is not a need for boot access.

Interview: Organizational personnel to determine that there is or is not a need for system boot access.

Related Controls:

AC-CMS-1(CMS-1) – Enhan	cement (High)	
Control		
	ot access to removable media drives is disabled.	
Applicability: All	References: ARS: AC-CMS-1(CMS-1)	Related Controls:
ASSESSMENT PROCEDUR	{E: AC-CMS-1(CMS-1).1	
Assessment Objective		
Determine if the organization	on evaluates the need for system boot access by removable media drives.	
Assessment Methods And	Objects	
	cess documentation to determine that, if not explicitly required, boot access to removable media d	
	personnel to determine that, if not explicitly required, boot access to removable media drives is dis	sabled.
· · · · · · · · · · · · · · · · · · ·	ample of workstations to determine if boot access to removable media drives is disabled.	
AC-CMS-1(CMS-2) – Enhan	ncement (High)	
Control		
System BIOS settings are I	locked and BIOS access is protected by password (see IA-5, Authenticator Management).	
Applicability: All	References: ARS: AC-CMS-1(CMS-2)	Related Controls: IA-5
ASSESSMENT PROCEDUR	₹E: AC-CMS-1(CMS-2).1	
Assessment Objective		
Determine if the organization	on controls access to the system BIOS when unauthorized personnel may be in physical proximity	y to the system.
Assessment Methods And	Objects	
	ocumentation to determine if System BIOS settings are locked and BIOS access is protected by p	
•	personnel to determine that, if not explicitly required, boot access to removable media drives is dis	
	ample of workstations by attempting to access the System BIOS. Ensure that access to the System	em BIOS is protected by password.
AC-CMS-1(CMS-3) – Enhan	cement (High)	
Control		
If not explicitly required, rer	movable media drive functionality is disabled.	
Applicability: All	References: ARS: AC-CMS-1(CMS-3)	Related Controls:
ASSESSMENT PROCEDUR	₹E: AC-CMS-1(CMS-3).1	
Assessment Objective		
	on disables removable media drive functionality If not explicitly required.	
Assessment Methods And	Objects	
	lia drive documentation to determine that, if not explicitly required, removable media drive functior	
	personnel to determine that, if not explicitly required, removable media drive functionality is disable	ed.
Test: Sample of Information	n system workstations to determine if removable media drive functionality is disabled.	

Awareness and Training (AT) – Operational

AT-1 – Security Awareness and Training Policy and Procedures (High)

Control

An IS AT program shall be developed, documented, and implemented effectively for all personnel, including contractors and any other users of CMS information and information systems. The IS AT program shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information, information systems, and networks.

Guidance

The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-16 and 800-50 provide guidance on security awareness and training. NIST SP 800-12 provides guidance on security policies and procedures.

	1; PISP: 4.2.1	
Applicability: All	References: ARS: AT-1; FISCAM: TSP-4.2.2; IRS-1075: 5.6.2.7#1.1-2, 6.1#1; NIST 800-53/53A: AT-	Related Controls:

ASSESSMENT PROCEDURE: AT-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security awareness and training policy and procedures;

(ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review security awareness and training policy and procedures; and

(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.

Interview: Organizational personnel with security awareness and training responsibilities.

ASSESSMENT PROCEDURE: AT-1.2

Assessment Objective

Determine if:

(i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with security awareness and training responsibilities.

AT-2 – Security Awareness (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS AT program shall be consistent with 5 CFR Part 930 (http://opm.gov/fedregis/2004/69-061404-32835-a.pdf) and the guidance provided in NIST SP 800-50.

Guidance

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	References: ARS: AT-2; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3; NIST 800-53/53A: AT-2; PISP: 4.2.2	Related Controls:
ASSESSMENT PROCEDURE: AT-2.1	·	

ASSESSMENT PROCEDURE: A1-2.

Assessment Objective

(i) the organization provides basic coourity or	verspace training to all information system upper (including managers and conjer systemitics) before system	izing appage to the system and when required	
by system changes;	vareness training to all information system users (including managers and senior executives) before author	izing access to the system and when required	
	(ii) the security awareness training is consistent with applicable regulations and NIST SP 800-50;		
(iii) the security awareness and training mate	rials address the specific requirements of the organization and the information systems to which personnel	have authorized access;	
(iv) the organization defines the frequency of			
	ty awareness training in accordance with organization-defined frequency, at least annually.		
Assessment Methods And Objects			
	olicy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate con	des of federal regulations; security awareness	
3	ng materials; information system security plan; other relevant documents or records. ing the general information system user community.		
AT-2(0) – Enhancement (High)			
Control			
	gers and senior executives) receive basic information security awareness training prior to accessing any sy	stem's information; when required by system	
Applicability: All	References: ARS: AT-2(0); FISCAM: TSP-3.3.1; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3, 6.2#1.1-2, 6.2#1.4, 6.2#2.1; NIST 800-53/53A: AT-2; PISP: 4.2.2	Related Controls:	
ASSESSMENT PROCEDURE: AT-2(0).1			
Assessment Objective			
-	irements as specified in the baseline control and the specific CMS requirements as prescribed in this ampli	fying enhancement to the baseline control.	
Assessment Methods And Objects			
	olicy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate con		
	ng materials; information system security plan (for organization-defined frequency of refresher security awa	reness training); other relevant documents or	
records.	ing the general information quatern upor community		
	ing the general information system user community.		
AT-2(CMS-1) – Enhancement (High)			
Control	verspeep of information acquirity issues and threats		
Applicability: All	wareness of information security issues and threats. References: ARS: AT-2(CMS-1); HIPAA: 164.308(a)(5)(ii)(A); IRS-1075: 5.6.2.7#1.3	Related Controls:	
ASSESSMENT PROCEDURE: AT-2(CMS-1		Related Controls.	
Assessment Objective			
	security awareness training to all information system users (including managers and senior executives) before	ore authorizing access to the system and when	
required by system changes.			
Assessment Methods And Objects			
Examine: Security awareness and training po and threats has been established.	olicy and procedures; other relevant documents or records to determine that a program to promote continui	ing awareness of information security issues	
Interview: Organizational personnel with security awareness and training responsibilities to determine that a program to promote continuing awareness of information security issues and threats has been established.			
AT-3 – Security Training (High)			
Control			
significant information system security respor	all positions and/or roles with significant information system security responsibilities during the system dev nsibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. ion systems to which personnel have authorized access. The employee shall acknowledge having received course completion.	Content of the security awareness training	
Guidance			
access. In addition, the organization provides	content of security training based on the specific requirements of the organization and the information systes system managers, system and network administrators, and other personnel having access to system-leve on's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C	I software, adequate technical training to	
Rev. 9	Page 33 of 207	BPSSM Appendix A. Attachment 1	

Applicability: All Reference	ces: ARS: AT-3; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	Related Controls:
ASSESSMENT PROCEDURE: AT-3.1		
Assessment Objective		
Determine if:		
	ormation system security responsibilities and documents those roles and responsibilities	
	with identified information system security roles and responsibilities before authorizing	access to the system or performing assigned duties
and when required by system changes;		
	and activities necessary to fulfill the organization-defined roles and responsibilities for in	nformation system security;
(iv) the security training is consistent with applicable regula		
(v) the organization defines the frequency of refresher secu		
	accordance with organization-defined frequency, at least annually.	
Assessment Methods And Objects	use addressing easurity training implementation, NICT CD 900 FO, and a of federal rea	
materials; information system security plan; other relevant	ares addressing security training implementation; NIST SP 800-50; codes of federal reg	julations; security training curriculum; security trainin
Interview: Organizational personnel with significant inform		
AT-3(0) – Enhancement (High)		
Control		
	as and responsibilities to undergo appropriate information system security training prior	to outborizing occord to CMS potworks, ovetema
and/or applications; when required by system changes; and	d refresher training every 365 days thereafter.	
Applicability: All Reference PISP: 4.2	ces: ARS: AT-3(0); FISCAM: TSP-3.3.1; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT- 2.3	3; Related Controls:
ASSESSMENT PROCEDURE: AT-3(0).1		
Assessment Objective		
Determine if the organization meets the requirements as sp	pecified in the baseline control and the specific CMS requirements as prescribed in this	amplifying enhancement to the baseline control.
Assessment Methods And Objects		
Examine: Security awareness and training policy; procedu	ares addressing security training implementation; NIST SP 800-50; codes of federal reg	ulations; security training curriculum; security trainir
	on-defined frequency of refresher security training); other relevant documents or records	δ.
Interview: Organizational personnel with significant inform	nation system security responsibilities.	
AT-4 – Security Training Records (High)		
Control		
	ented effectively to ensure that individual IS training activities, including basic security a	awareness training and specific information system
security training, are properly documented and monitored.		
Guidance		
Procedures and training implementation should:	responsibilities and provide role specific training in accordance with National Institute a	of Standarda and Tachnalamy (NIST) atondarda and
quidance:	responsibilities and provide role-specific training in accordance with National Institute c	of Standards and Technology (NIST) standards and
0	d to security awareness materials at least annually. Users of CMS information systems	include employees, contractors, students, quest
researchers, visitors, and others who may need access to		
	basics and policy level training in security planning and management.	
	g in information security basics; management and implementation level training in secu	
	training in system/ application life cycle management, risk management, and continger	
	managers, auditors, and other security-oriented personnel (e.g., system and network ac	
management, and contingency planning.	s and broad training in security planning, system and application security management	, system/application life cycle management, fisk
	st receive training in information security basics; management and implementation leve	I training in security planning and system/applicatio
	ion level training in system/ application life cycle management, risk management, and c	
	ess material/exposure outlined in NIST guidance on IT security awareness and training	
the systems.		-
(c) Provide information systems security refresher training	for employees as frequently as determined necessary, based on the sensitivity of the i	
Rev. 9	Page 34 of 207	BPSSM Appendix A, Attachmen

(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.				
Applicability: All	References: ARS: AT-4; FISCAM: TSP-4.2.3; IRS-1075: 6.2#1.3; NIST 800-53/53A: AT-4; PISP: 4.2.4	Related Controls:		
ASSESSMENT PROCEDURE: AT-4.1				
Assessment Objective				
Determine if the organization monitors and doc	uments basic security awareness training and specific information system security training.			
Assessment Methods And Objects				
Examine: Security awareness and training pol	cy; procedures addressing security training records; security awareness and training records; other relevant	ant documents or records.		
AT-5 – Contacts with Security Groups	and Associations (High)			
Control				
Contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations shall be encouraged and supported to enable security personnel to stay up to date with the latest recommended security practices, techniques, and technologies; and to share the latest security-related information including threats, vulnerabilities, and incidents.				
Guidance				
To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.				
Applicability: All	References: ARS: AT-5; HSPD 7: H(25); NIST 800-53/53A: AT-5; PISP: 4.2.5	Related Controls:		
ASSESSMENT PROCEDURE: AT-5.1				
Assessment Objective Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security				
techniques and technologies and to share security-related information.				
Assessment Methods And Objects				
Examine: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information				

system security knowledge, expertise, and general information; other relevant documents or records.(Optional)

Audit and Accountability (AU) – Technical

AU-1 – Audit and Accountability Policy and Procedures (High)	
Control	
All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Pr	
implementation and management of audit controls, and shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, stand	ards, and guidance; and shall be reviewed
periodically, and, if necessary, updated.	
Guidance	
The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and	
policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the	e security program in general, and for a
particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.	
Applicability: All References: ARS: AU-1; IRS-1075: 5.6.3.3#1; NIST 800-53/53A: AU-1; PISP: 4.3.1	Related Controls:
ASSESSMENT PROCEDURE: AU-1.1	
Assessment Objective	
Determine if:	
(i) the organization develops and documents audit and accountability policy and procedures;	
(ii) the organization disseminates audit and accountability policy and procedures to appropriate elements within the organization;	
(iii) responsible parties within the organization periodically review audit and accountability policy and procedures; and	
(iv) the organization updates audit and accountability policy and procedures when organizational review indicates updates are required.	
Assessment Methods And Objects	
Examine: Audit and accountability policy and procedures; other relevant documents or records.	
Interview: Organizational personnel with audit and accountability responsibilities.	
ASSESSMENT PROCEDURE: AU-1.2	
Assessment Objective	
Determine if:	
(i) the audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizationa	
(ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations	
(iii) the audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant imple	ementations of all associated security
controls.	
Assessment Methods And Objects	
Examine: Audit and accountability policy and procedures; other relevant documents or records.	
Interview: Organizational personnel with audit and accountability responsibilities.	
AU-2 – Auditable Events (High)	
Control	
Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to sup	
incidents. The selection of auditable events shall be based upon a risk assessment as to which events require auditing on a continuous basis, and which	events require auditing in response to
specific situations.	
Guidance	
The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. T	
system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based	
auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of al information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilit	
problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support be	
information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig/cig.html provide recommended lists of au	
auditable events that are adequate to support after-the-fact investigations of security incidents. NIST SP 800-92 provides guidance on computer security	
Applicability: All References: ARS: AU-2; FISCAM: TAC-4.3.4, TSD-3.2.2; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b);	Related Controls: AU-4
IRS-1075: 5.6.3.3#2.1: NIST 800-53/53A: AU-2: PISP: 4.3.2	

ASSESSMENT PROCEDURE: AU-2.1		
Assessment Objective		
Determine if:		
(i) the organization defines information system	auditable events:	
	e adequate to support after-the-fact investigations of security incidents; and	
	ords for the organization-defined auditable events.	
Assessment Methods And Objects		
	edures addressing auditable events; information system security plan; information system configuration se	ettings and associated documentation.
information system audit records; other relevar	t documents or records.	
	formation system auditing of organization-defined auditable events.	
AU-2(0) – Enhancement (High)		
Control		
Generate audit records for the following events		
(a) User account management activities,		
(b) System shutdown,		
(c) System reboot,		
(d) System errors,		
(e) Application shutdown,		
(f) Application restart, (g) Application errors,		
(g) Application errors, (h) File creation,		
(i) File deletion,		
(i) File modification,		
(k) Failed and successful log-ons,		
(I) Security policy modifications,		
(m) Use of administrator privileges, and		
(n) File access.		
Guidance		
	llowing events in addition to those specified in other controls:	
(a) All successful and unsuccessful authorization		
(b) All changes to logical access control author	ities (e.g., rights, permissions).	
(c) All system changes with the potential to cor	npromise the integrity of audit policy configurations, security policy configurations and audit record genera	tion services.
(d) The audit trail shall capture the enabling or	disabling of audit report generation services.	
	hanges, batch file changes and queries made to the system (e.g., operating system, application, and data	
Applicability: All	References: ARS: AU-2(0); FISCAM: TAC-2.1.5, TAC-4.1, TSD-3.2.4; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3; NIST 800-53/53A: AU-2; PISP: 4.3.2	Related Controls:
ASSESSMENT PROCEDURE: AU-2(0).1	104.312(b), INO-1073. 3.0.3.3#2.1, 3.0.3.3#6, NIGT 000-33/35A. A0-2, ITOF . 4.3.2	
Assessment Objective		
•	ments as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ving enhancement to the baseline control
Assessment Methods And Objects	intents as specified in the baseline control and the specific Civio requirements as prescribed in this amplifi	ying enhancement to the baseline control.
	edures addressing auditable events; information system security plan (for list of organization-defined audi	table events): information system
	tation; information system audit records; other relevant documents or records.	
	formation system audit records, other relevant documents of records.	
AU-2(1) – Enhancement (High)		
Control		
	from multiple components throughout the system into a system-wide (logical or physical) time correlated a	audit trail.
Applicability: All	References: ARS: AU-2(1); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2(1)	Related Controls:

ASSESSMENT PROCEDURE: AU-2(1).1		
Assessment Objective		
Determine if:		
	e information system that generate audit records; and	
	s from the organization-defined (multiple) components within the information system into a systemwi	de (logical or physical), time-correlated audit trail.
Assessment Methods And Objects		(-3
•	dures addressing auditable events; information system design documentation; information system co	nfiguration settings and associated
documentation; list of organization-defined audit	able events; information system audit records; other relevant documents or records.	
Test: Automated mechanisms implementing a s	ystem-wide auditing capability.	
AU-2(2) – Enhancement (High)		
Control		
Provide the capability to manage the selection o	f events to be audited by individual components of the information system.	
Applicability: All	References: ARS: AU-2(2); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2(2)	Related Controls:
ASSESSMENT PROCEDURE: AU-2(2).1		
Assessment Objective		
	capability to manage the selection of events to be audited by individual components of the system.	
Assessment Methods And Objects		
	dures addressing auditable events; information system design documentation; information system co	nfiguration settings and associated
	able events; information system audit records; other relevant documents or records.	
	ormation system auditing for the specified components of the information system.	
AU-2(3) – Enhancement (High)		
Control		
Periodically review and update the list of auditab		
	References: ARS: AU-2(3); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2(3)	Related Controls:
ASSESSMENT PROCEDURE: AU-2(3).1		
Assessment Objective		
	s and updates the list of organization-defined auditable events.	
Assessment Methods And Objects		
other relevant documents or records.	dures addressing auditable events; list of organization-defined auditable events; information system	audit records; information system incident reports;
Interview: Organizational personnel with auditin	a and accountability responsibilities	
AU-2(CMS-1) – Enhancement (High)		
Control		
Enable logging for perimeter devices, including f	irewalls and routers	
(a) Log packet screening denials originating from		
(b) Packet screening denials originating from true		
(c) User account management,		
(d) Modification of proxy services,		
(e) Application errors,		
(f) System shutdown and reboot,(g) System errors,		
(b) Modification of proxy services, and		
(i) Modification of packet filters.		
Applicability: All	References: ARS: AU-2(CMS-1); HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	Related Controls:
ASSESSMENT PROCEDURE: AU-2(CMS-1).1		
Assessment Objective		
Determine if:		

	(i) the organization defines information	tion system auditable events;	
--	--	-------------------------------	--

- (ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and
 (iii) the information system generates audit records for the organization-defined auditable events.
 Assessment Methods And Objects

Assessment Methous And		
Examine: Audit and accou	untability policy; procedures addressing auditable events; information system security plan (for list of organization-defined aud	litable events); information system
	associated documentation; information system audit records; other relevant documents or records to determine if logging-on i	is enabled for perimeter devices, including
	s logging will capture the following information:	
	denials originating from un-trusted networks,	
(b) packet screening denia	als originating from trusted networks,	
(c) user account managem		
(d) modification of proxy set	ervices,	
(e) application errors,		
(f) system shutdown and re	eboot,	
(g) system errors,		
(h) modification of proxy se		
(i) modification of packet fi		
	personnel with audit and accountability responsibilities to determine if logging-on is enabled for perimeter devices, including fi	irewalls and routers. This logging will capture
the following information:		
	denials originating from un-trusted networks,	
	als originating from trusted networks,	
(c) user account managem		
(d) modification of proxy se	ervices,	
(e) application errors,		
(f) system shutdown and re	eboot,	
(g) system errors,		
(h) modification of proxy se		
(i) modification of packet fi		
	isms implementing information system auditing of organization-defined auditable events.	
AU-2(CMS-2) – Enhancem	ent (High)	
Control		
Verify that proper logging i	is enabled in order to audit administrator activities.	
Applicability: All	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	Related Controls:
ASSESSMENT PROCEDUI	RE: AU-2(CMS-2).1	
Assessment Objective		
-	on system generates audit records for the organization-defined auditable events.	
Assessment Methods And		
	•	
	untability policy; procedures addressing auditable events; information system security plan (for list of organization-defined aud	
	associated documentation; information system audit records; other relevant documents or records to determine if proper logg	ing is enabled in order to audit administrator
activities.		ininter a stilling
•	personnel with account audit and accountability responsibilities to determine if proper logging is enabled in order to audit adm	inistrator activities.
	isms implementing information system auditing of organization-defined auditable events.	
AU-3 – Content of Audit	t Records (High)	
Control		
Automated mechanisms sl	hall be established to provide the capability to include specific information in audit records. Audit records shall contain sufficie	ent information to establish what events
	s occurred, the source of the events, the cause of the events, and the event outcome.	
Guidance		
	deal for most sudit reporter (i) data and time of the supert; (ii) the component of the information system (a.g. coftware component	ant bardwara companent) where the event
	des, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component of the system to the system of the sys	
	t; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST SP 800-92 provides guidance on comp	
Applicability: All	References: ARS: AU-3; FISCAM: TAC-3.2.D.1, TAN-2.1.9; IRS-1075: 5.6.3.3#3; NIST 800-53/53A:	Related Controls:
Day 0	Deces 20 of 207	DDSSM Amondin A Attachment 1
Rev. 9	Page 39 of 207	BPSSM Appendix A, Attachment 1

AU-3: PISP: 4.3.3	
ASSESSMENT PROCEDURE: AU-3.1	
Assessment Objective	
Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the out	comes of the events.
Assessment Methods And Objects	
Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information syste reports; other relevant documents or records.	em audit records; information system incident
Test: Automated mechanisms implementing information system auditing of auditable events.	
AU-3(1) – Enhancement (High)	
Control	
Provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	
Applicability: All References: ARS: AU-3(1); NIST 800-53/53A: AU-3(1)	Related Controls:
ASSESSMENT PROCEDURE: AU-3(1).1	
Assessment Objective	
Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified	by type, location, or subject.
Assessment Methods And Objects	
Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; information system	n security plan; information system
configuration settings and associated documentation; other relevant documents or records.	
Test: Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject.	
AU-3(2) – Enhancement (High)	
Control	
Centrally manage the content of audit records generated by individual components throughout the system.	
Applicability: All References: ARS: AU-3(2); NIST 800-53/53A: AU-3(2)	Related Controls:
ASSESSMENT PROCEDURE: AU-3(2).1	
Assessment Objective	
Determine if the information system provides the capability to centrally manage the content of audit records generated from multiple components through	nout the system.
Assessment Methods And Objects	
Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; list of organization	-defined auditable events; information system
configuration settings and associated documentation; information system audit records; other relevant documents or records.	
Test: Automated mechanisms implementing information system auditing with central management capability.	
AU-3(CMS-1) – Enhancement (High)	
Control	
Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and re extract that the data is erased or its use is still required.	eleasing party. Verify every 90 days for each
Applicability: All References: ARS: AU-3(CMS-1); FISCAM: TAC-4.1; HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.2	Related Controls:
ASSESSMENT PROCEDURE: AU-3(CMS-1).1	
Assessment Objective	
Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the out	comes of the events.
Assessment Methods And Objects	
Examine: Audit and accountability policy; procedures addressing the content of audit records; list of organization-defined auditable events; information s incident reports; other relevant documents or records to determine if the organization records disclosures of sensitive information, including protected he organization must log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its Interview: Organizational personnel with account audit and accountability responsibilities to determine if the organization records disclosures of sensitive financial information. The organization must log information type, date, time, receiving party, and releasing party, and releasing party. Verify every 90 days for each extract the Test: Automated mechanisms implementing information system auditing of auditable events with organization-defined audit record content.	alth and financial information. The success and set of the set of

AU-4 – Audit Storage Capacity (High)		
Control		
	e capacity shall be allocated for audit records, and information systems shall be configure	ed to reduce the likelihood of audit records exceeding such
Guidance		
The organization provides sufficient audit storage	capacity, taking into account the auditing to be performed and the online audit processi	ng requirements.
Applicability: All	References: ARS: AU-4; IRS-1075: 5.6.3.3#4; NIST 800-53/53A: AU-4; PISP: 4.3.4	Related Controls: AU-2, AU-5, AU-6, AU- 7, SI-4
ASSESSMENT PROCEDURE: AU-4.1		
Assessment Objective Determine if: (i) the organization defines audit record storage of (ii) the organization establishes information syste Assessment Methods And Objects Examine: Audit and accountability policy; proceed system components generating audit records; list	apacity for the information system components that generate audit records; and m configuration settings to reduce the likelihood of the audit record storage capacity beir ures addressing audit storage capacity; information system design documentation; orga of organization-defined auditable events; information system configuration settings and	nization-defined audit record storage capacity for information
other relevant documents or records.		
AU-5 – Response to Audit Processing Fa	ailures (High)	
Control		
Automated mechanisms shall be established whi reached and to take appropriate additional actior	ch provide the capability to generate information system alerts for appropriate officials in s.	the event of an audit failure or audit storage capacity being
Guidance		
Audit processing failures include, for example, so	ftware/hardware errors, failures in the audit capturing mechanisms, and audit storage ca	apacity being reached or exceeded.
Applicability: All	References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5	Related Controls: AU-4
ASSESSMENT PROCEDURE: AU-5.1		
Assessment Methods And Objects Examine: Audit and accountability policy; proceed system configuration settings and associated door records.		nentation; information system security plan; information
	ctions in response to an audit failure or audit storage capacity issue: storage media is unavailable.	
Applicability: All	References: ARS: AU-5(0); NIST 800-53/53A: AU-5; PISP: 4.3.5	Related Controls:
ASSESSMENT PROCEDURE: AU-5(0).1		
Assessment Objective		
Determine if the organization meets the requirem Assessment Methods And Objects	ents as specified in the baseline control and the specific CMS requirements as prescribe	ed in this amplifying enhancement to the baseline control.
Examine: Audit and accountability policy; proceed	ures addressing response to audit processing failures; information system design docun	nentation; information system security plan (for list of actions

Test: Automated mechanisms implementing inf	prmation system response to audit processing failures.	
AU-5(1) – Enhancement (High)		
Control		
	n allocated audit record storage volume reaches 80% of audit record storage capacity.	
Applicability: All	References: ARS: AU-5(1); NIST 800-53/53A: AU-5(1)	Related Controls:
SSESSMENT PROCEDURE: AU-5(1).1		
ssessment Objective		
Determine if:		
(i) the organization defines percentage of maxim	um audit record storage capacity; and	
(ii) the information system provides a warning w	hen the allocated audit record storage volume reaches the organization-defined percentage of maximun	n audit record storage capacity.
ssessment Methods And Objects		
	dures addressing response to audit processing failures; information system design documentation; infor	mation system security plan; information
, , ,	cumentation; information system audit records; other relevant documents or records.	
Test: Automated mechanisms implementing auto	lit storage limit warnings.	
U-5(2) – Enhancement (High)		
Control		
A second real-time alert is sent when the audit r		
	References: ARS: AU-5(2); NIST 800-53/53A: AU-5(2)	Related Controls:
SSESSMENT PROCEDURE: AU-5(2).1		
ssessment Objective		
Determine if:		
(i) the organization defines audit failure events r		
	lert when organization-defined audit failure events occur.	
ssessment Methods And Objects		
	dures addressing response to audit processing failures; information system design documentation; infor	mation system security plan; information
	cumentation; information system audit records; other relevant documents or records.	
Test: Automated mechanisms implementing rea		
U-6 – Audit Monitoring, Analysis, and	Reporting (High)	
Control		
	red and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and/or suspicious	s activity. Such activity shall be investigate
and reported to appropriate officials, in accordar	ce with current CMS Procedures.	
and reported to appropriate officials, in accordar Guidance		
and reported to appropriate officials, in accordar Guidance Organizations increase the level of audit monitor	ing and analysis activity within the information system whenever there is an indication of increased risk	to organizational operations, organizationa
and reported to appropriate officials, in accordan Guidance Organizations increase the level of audit monito assets, or individuals based on law enforcement	ing and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information.	
and reported to appropriate officials, in accordan Guidance Organizations increase the level of audit monito assets, or individuals based on law enforcement	ring and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D),	to organizational operations, organizationa Related Controls: AU-4, IR-4
and reported to appropriate officials, in accordan Suidance Organizations increase the level of audit monitor assets, or individuals based on law enforcement Applicability: All	ing and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information.	
and reported to appropriate officials, in accordan Guidance Organizations increase the level of audit monitor assets, or individuals based on law enforcement Applicability: All ASSESSMENT PROCEDURE: AU-6.1	ring and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D),	
and reported to appropriate officials, in accordan and reported to appropriate officials, in accordan assets, or individuals based on law enforcement pplicability: All SSESSMENT PROCEDURE: AU-6.1 ssessment Objective	ring and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D),	
and reported to appropriate officials, in accordan Suidance Organizations increase the level of audit monito assets, or individuals based on law enforcement pplicability: All SSESSMENT PROCEDURE: AU-6.1 SSESSMENT Objective Determine if:	ring and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6	
and reported to appropriate officials, in accordar Guidance Organizations increase the level of audit monito assets, or individuals based on law enforcement Applicability: All ASSESSMENT PROCEDURE: AU-6.1 Assessment Objective Determine if: (i) the organization regularly reviews/analyzes a	ing and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6	
and reported to appropriate officials, in accordar Suidance Organizations increase the level of audit monito assets, or individuals based on law enforcement pplicability: All SSESSMENT PROCEDURE: AU-6.1 Sessment Objective Determine if: (i) the organization regularly reviews/analyzes a (ii) the organization investigates suspicious activ	ing and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6	
and reported to appropriate officials, in accordar iuidance Organizations increase the level of audit monito assets, or individuals based on law enforcement pplicability: All SSESSMENT PROCEDURE: AU-6.1 ISSESSMENT Objective Determine if: (i) the organization regularly reviews/analyzes a (ii) the organization investigates suspicious activ (iii) the organization reports findings of inapprop	ing and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6 udit records for indications of inappropriate or unusual activity; ity or suspected violations; riate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and	
and reported to appropriate officials, in accordar Suidance Organizations increase the level of audit monito assets, or individuals based on law enforcement applicability: All SSESSMENT PROCEDURE: AU-6.1 Seessment Objective Determine if: (i) the organization regularly reviews/analyzes a (ii) the organization investigates suspicious activ (iii) the organization reports findings of inapprop (iv) the organization takes necessary actions in	ing and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6	
and reported to appropriate officials, in accordar Guidance Organizations increase the level of audit monito assets, or individuals based on law enforcement Applicability: All ASSESSMENT PROCEDURE: AU-6.1 Assessment Objective Determine if: (i) the organization regularly reviews/analyzes a (ii) the organization reports findings of inapprop (iv) the organization takes necessary actions in Assessment Methods And Objects	ing and analysis activity within the information system whenever there is an indication of increased risk information, intelligence information, or other credible sources of information. References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6 udit records for indications of inappropriate or unusual activity; ity or suspected violations; riate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and	Related Controls: AU-4, IR-4

	ecords. ring, analysis, and reporting capability.	
ASSESSMENT PROCEDURE: AU-6.2		
Assessment Objective		
	s the level of audit monitoring and analysis activity whenever there is increased risk to organiza	ational operations and assets, or to individuals, based on
	anizations, the intelligence community, or other credible sources.	
Assessment Methods And Objects		
Examine: Audit and accountability pol	icy; procedures addressing audit monitoring, analysis, and reporting; threat information docume	entation from law enforcement, intelligence community, or othe
· · · · · ·	tion settings and associated documentation; information system audit records; other relevant do	ocuments or records.
	ith information system audit monitoring, analysis, and reporting responsibilities.	
AU-6(1) – Enhancement (High)		
Control		
Employ automated mechanisms to inte	egrate audit monitoring, analysis, and reporting into an overall process for investigation and res	ponse to suspicious activities.
Applicability: All	References: ARS: AU-6(1); HIPAA: 164.312(b); NIST 800-53/53A: AU-6(1)	Related Controls:
ASSESSMENT PROCEDURE: AU-6(i).1	
Assessment Objective		
Determine if the organization employs	automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall provide the second sec	ocess for investigation and response to suspicious activities.
Assessment Methods And Objects		
Examine: Audit and accountability pol associated documentation; other relev	icy; procedures addressing audit monitoring, analysis, and reporting; information system design	n documentation; information system configuration settings an
	ting audit monitoring, analysis, and reporting into an organizational process for investigation and	d response to suspicious activities
AU-6(2) – Enhancement (High)		d response to suspicious activities.
Control		The set of the second
	nediately alert security personnel of the following minimal examples of inappropriate or unusua nsitive data; and threats to finances, personnel, or property.	a activities with security implications: threats to infrastructure,
Applicability: All	References: ARS: AU-6(2); HIPAA: 164.312(b); NIST 800-53/53A: AU-6(2)	Related Controls:
ASSESSMENT PROCEDURE: AU-6(2		Related Controls.
Assessment Objective	·/··	
Determine if:		
	te or unusual activities with security implications; and	
	d mechanisms to alert security personnel of the occurrence of any organization-defined inappro	opriate or unusual activities with security implications.
Assessment Methods And Objects	, , , , , , , , , , , , , , , , , , ,	· · · · · · · · · · · · · · · · · · ·
	icy; procedures addressing audit monitoring, analysis, and reporting; information system desigr	n documentation; information system configuration settings an
	system security plan; information system audit records; other relevant documents or records.	
Test: Automated mechanisms implem	enting security alerts.	
AU-6(CMS-1) – Enhancement (High)		
Control		
Review system records for initialization	n sequences, log-ons and errors; system processes and performance; and system resources ut	tilization to determine anomalies on demand but no less than
once within a twenty-four (24) hour pe	riod. Generate alert notification for technical staff review and assessment.	
Applicability: All	References: ARS: AU-6(CMS-1); FISCAM: TAC-4.2	Related Controls:
ASSESSMENT PROCEDURE: AU-6(CMS-1).1	
Assessment Objective		
Determine if:		
	analyzes audit records for indications of inappropriate or unusual activity;	
(ii) the organization investigates suspi	cious activity or suspected violations;	
(iii) the organization reports findings of		iolo: and
	i inappropriate/usual activities, suspicious behavior, or suspected violations to appropriate offici	
	r inappropriate/usual activities, suspicious behavior, or suspected violations to appropriate offici actions in response to the reviews/analyses of audit records.	ais, aiu

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Interview: Organizational personnel responsible for audit and accountability to determine if initialization sequences, log-ons and errors; system processes and performance; and system resource utilization are recorded to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment. Test: Information system audit monitoring, analysis, and reporting capability to determine if initialization sequences, log-ons and errors; system processes and performance; and system resource utilization are recorded to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

AU-6(CMS-2) – Enhancement (High)

Control

Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.

Applicability: All	References: ARS: AU-6(CMS-2)	Related Controls:		
ASSESSMENT PROCEDURE: AU-6(CMS-2).1				
Assessment Objective				
Determine if the organization regularly reviews /	analyzes audit records for indications of inappropriate or unusual activity.			
Assessment Methods And Objects				
	dures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions ta			
	r initialization sequences, log-ons and errors; system processes and performance; and system resources			
alerts for technical staff review and assessment.	d border defense devices are reviewed to determine anomalies on demand but no less than once within	a twenty-lour (24) hour period. Generate		
	e for audit and accountability to determine if network traffic, bandwidth utilization rates, alert notifications,	and border defense devices are reviewed to		
	n once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.			
	rsis, and reporting capability to determine if network traffic, bandwidth utilization rates, alert notifications	, and border defense devices are reviewed to		
	n once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment.			
AU-6(CMS-3) – Enhancement (High)				
Control				
	tions on the information system, report findings to appropriate officials and take appropriate action.			
Applicability: All	References: ARS: AU-6(CMS-3); FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.3, TAC-4.3.4; HIPAA: 164.312(b)	Related Controls:		
ASSESSMENT PROCEDURE: AU-6(CMS-3).1				
Assessment Objective				
Determine if the organization investigates suspic	cious activity or suspected violations.			
Assessment Methods And Objects				
	dures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions ta			
	records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action.			
o	e for audit and accountability to determine if the organization investigates suspicious activity or suspected			
reports findings to appropriate officials and takes		a violationo on the information system, and		
· · · · ·	sis, and reporting capability to determine if the organization investigates suspicious activity or suspected	d violations on the information system, and		
reports findings to appropriate officials and takes	s appropriate action.			
AU-6(CMS-4) – Enhancement (High)				
Control				
	nce daily for unusual, unexpected, or suspicious behavior.	1		
Applicability: All	References: ARS: AU-6(CMS-4); HIPAA: 164.312(b)	Related Controls:		
ASSESSMENT PROCEDURE: AU-6(CMS-4).1				
Assessment Objective				
Determine if the organization employs automate	d mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigat	on and response to suspicious activities		

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

Interview: Organizational personnel responsible for audit and accountability to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

Test: Information system audit monitoring, analysis, and reporting capability to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior.

AU-6(CMS-5) – Enhancement (High)

Control

Inspect administrator groups on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Applicability: All	References: ARS: AU-6(CMS-5); FISCAM: TAC-2.1.5; HIPAA: 164.312(b)	Related Controls:

ASSESSMENT PROCEDURE: AU-6(CMS-5).1

Assessment Objective

Determine if the organization monitors activities of system administrators.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Interview: Organizational personnel with audit and accountability responsibilities to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

Test: Information system audit monitoring, analysis, and reporting capability to determine if administrator groups are inspected on demand but at least once every seven (7) days to ensure unauthorized administrator accounts have not been created.

AU-6(CMS-6) – Enhancement (High)

Control

Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Applicability: All References: ARS: AU-6(CMS-6); HIPAA: 164.312(b)

ASSESSMENT PROCEDURE: AU-6(CMS-6).1

Assessment Objective

Determine if the organization randomly performs a manual review of automated audit systems to validate the correctness of the automated system.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Interview: Organizational personnel with audit and accountability responsibilities to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

Test: Information system audit monitoring, analysis, and reporting capability to determine if the organization performs manual reviews of system audit records randomly on demand but at least once every thirty (30) days.

AU-6(FIS-1) – Enhancement (High)

Control

The use of privileged system software and utilities is reviewed by technical management. Systems programmers' activities are monitored and reviewed. Inappropriate or unusual activity in using utilities is investigated.

Applicability: All	References: FISCAM: TSS-2.2.1, TSS-2.2.2, TSS-2.2.3	Related Controls:
ASSESSMENT PROCEDURE: AU-6(FIS-1).1		

Assessment Objective

Determine if the organization monitors and reviews system programmers' activities and investigates inappropriate or unusual activities when using privileged system software utilities.

Related Controls:

Assessment Methods And Objects		
Examine: Documentation supporting the supervising and monitoring of systems programmers' activities.		
Examine: Documentation supporting their review		
Examine: Documentation supporting these invest	stigations.	
Examine: Pertinent policies and procedures.		
	determine their activities related to supervising and monitoring their staff.	
	ir reviews of privileged system software and utilities usage.	
AU-6(IRS-1) – Enhancement (High)		
Control		
	ling receipt and/or disposal of returns or return information, shall be maintained in a log. (see IRS Pub.	1075, sect 6.3.1)
Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	References: IRS-1075: 6.3.1#1	Related Controls:
ASSESSMENT PROCEDURE: AU-6(IRS-1).1		
Assessment Objective		
	all requests for returned FTI, and the log includes receipt and/or disposal of returns (see IRS Pub. 1075	i, sect 6.3.1).
Assessment Methods And Objects		
Examine: Logs for requests of FTI include receip	ot and/or disposal or FTI information is returned.	
	ling FTI to determine is there is an effective log of FTI requests, disposal or returns.	
AU-7 – Audit Reduction and Report Gen		
Control		
	supporting procedures shall be developed, documented, and implemented effectively to enable human	n review of audit information and the
generation of appropriate audit reports.		
Guidance		
· • • • • • • • • • • • • • • • • • • •	ort after-the-fact investigations of security incidents without altering original audit records.	
Applicability: All	References: ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7	Related Controls: AU-4
ASSESSMENT PROCEDURE: AU-7.1		
Assessment Objective		
Determine if the information system provides an	audit reduction and report generation capability.	
Assessment Methods And Objects		
Examine: Audit and accountability policy; proceed information system audit records; other relevant	lures addressing audit reduction and report generation; information system design documentation; audi documents or records.	t reduction, review, and reporting tools;
Interview: Organizational personnel with informa	ation system audit monitoring, analysis, and reporting responsibilities.	
Test: Audit reduction and report generation capa	bility.	
AU-7(1) – Enhancement (High)		
Control		
Employ a system capability that automatically pro	ocesses audit records for events of interest based upon selectable, event criteria.	
Applicability: All	References: ARS: AU-7(1); NIST 800-53/53A: AU-7(1)	Related Controls:
ASSESSMENT PROCEDURE: AU-7(1).1		
Assessment Objective		
	capability to automatically process audit records for events of interest based upon selectable, event cri	teria.
Assessment Methods And Objects		
	lures addressing audit reduction and report generation; information system design documentation; infor	mation system configuration settings and
	w, and reporting tools; information system audit records; other relevant documents or records.	mation system configuration settings and
Test: Audit reduction and report generation capa		

AU-8 – Time Stamps (High)		
Control		
Audit records shall employ time stamps for us	e in audit record generation. Time stamps of audit records shall be generated using ir	nternal system clocks that are synchronized system-wide.
Guidance		
Time stamps (including date and time) of audi	t records are generated using internal system clocks.	
Applicability: All	References: ARS: AU-8; NIST 800-53/53A: AU-8; PISP: 4.3.8	Related Controls:
ASSESSMENT PROCEDURE: AU-8.1		
Assessment Objective		
Determine if the information system provides	time stamps for use in audit record generation.	
Assessment Methods And Objects		
Examine: Audit and accountability policy; pro documentation; information system audit reco	cedures addressing time stamp generation; information system design documentation rds; other relevant documents or records.	; information system configuration settings and associated
Test: Automated mechanisms implementing t	ime stamp generation.	
AU-8(1) – Enhancement (High)		
Control		
Information system clock synchronization occ	urs daily and at system boot.	
Applicability: All	References: ARS: AU-8(1); NIST 800-53/53A: AU-8(1)	Related Controls:
ASSESSMENT PROCEDURE: AU-8(1).1		
Assessment Objective		
Determine if:		
	ternal clock synchronization for the information system; and	
	rmation system clocks periodically in accordance with organization-defined frequency.	
Assessment Methods And Objects		
Examine: Audit and accountability policy; pro	cedures addressing time stamp generation; information system security plan; informat	tion system design documentation; information system
configuration settings and associated docume		
· · · · · · · · · · · · · · · · · · ·	nternal information system clock synchronization.	
AU-9 – Protection of Audit Information	n (rign)	
Control		
· · · · · · · · · · · · · · · · · · ·	ected from unauthorized access, modification, and deletion.	
Guidance		
	, audit records, audit settings, and audit reports) needed to successfully audit informat	
	References: ARS: AU-9; NIST 800-53/53A: AU-9; PISP: 4.3.9	Related Controls:
ASSESSMENT PROCEDURE: AU-9.1		
Assessment Objective		
	audit information and audit tools from unauthorized access, modification, and deletion.	
Assessment Methods And Objects		
configuration settings and associated docume	cedures addressing protection of audit information; access control policy and procedure entation, information system audit records; audit tools; other relevant documents or rec	
Test: Automated mechanisms implementing a	audit information protection.	
AU-9(1) – Enhancement (High)		
Control		
	icted to hardware-enforced, "write-once" media for recording audit information (e.g., C	
Applicability: All	References: ARS: AU-9(1); NIST 800-53/53A: AU-9(1)	Related Controls:

ASSESSMENT PROCEDURE: AU-9(1).1

Assessment Objective

Determine if the information system produces audit information on hardware-enforced, write-once media.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; other relevant documents or records.(Optional)
Test: Media storage devices.(Optional)

AU-10 – Non-Repudiation (High)

Control

Non-repudiation mechanisms shall be implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message.

Guidance

Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Applicability: All	References: ARS: AU-10; NIST 800-53/53A: AU-10; PISP: 4.3.10	Related Controls:

ASSESSMENT PROCEDURE: AU-10.1

Assessment Objective

Determine if the information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing non-repudiation capability.(Optional)

AU-11 – Audit Record Retention (High)

Control

Audit records shall be retained to provide support for after-the-fact investigations of security incidents, and to meet regulatory and/or CMS information retention requirements. The National Archives and Records Administration maintains criteria for record retention across many disciplines and information security retention standards shall not be construed to relieve or waive these other standards.

Guidance

The organization retains audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions (CMS sensitive information retention). Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST SP 800-61 provides guidance on computer security incident handling and audit record retention.

Applicability: All	References: NIST 800-53/53A: AU-11	Related Controls:
ASSESSMENT PROCEDURE: AU-11.1		

Assessment Objective

Determine if:

(i) the organization defines the retention period for audit records generated by the information system; and

(ii) the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information system audit record retention responsibilities.

Control		
Control	dave, and archive old audit records. Betain audit record archives for one (1) year	
Applicability: All	days, and archive old audit records. Retain audit record archives for one (1) year. References: ARS: AU-11(0); NIST 800-53/53A: AU-11; PISP: 4.3.11	Related Controls:
		Related Controls.
Assessment Objective	the requirements on appendiced in the baseline control and the appendice CMS requirements on preserve	ribad in this amplifying aphanaamant to the baseline control
Assessment Methods And Object	the requirements as specified in the baseline control and the specific CMS requirements as prescr	ibed in this amplifying enhancement to the baseline control.
	olicy; procedures addressing audit record retention; organization-defined retention period for audit	records: information system audit records: other relevant
documents or records.		
Interview: Organizational personne	l with information system audit record retention responsibilities.	
AU-11(PII-1) – Enhancement (High		
Control	,	
Employ mechanisms to facilitate the	e review of PII disclosure/access records and retain the records for five (5) years or the applicable r	ecords control schedule, whichever is longer.
Applicability: All	References: IRS-1075: 3.1#1	Related Controls:
ASSESSMENT PROCEDURE: AU-	11(PII-1).1	
Assessment Objective		
•	ys mechanisms to facilitate the review of PII disclosures/access records and retains the records for	r five (5) years or the applicable records control schedule,
whichever is longer.		
Assessment Methods And Object		
Examine: PII disclosure/access aud	lit records are retained or a control schedule indicates (5) five years or longer.	
	lit records are retained or a control schedule indicates (5) five years or longer.	
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control	dit records are retained or a control schedule indicates (5) five years or longer.)	
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all	dit records are retained or a control schedule indicates (5) five years or longer.) organizations must ensure that audit information is archived for six (6) years to enable the recreati	on of computer-related accesses to both the operating system
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII	dit records are retained or a control schedule indicates (5) five years or longer.) organizations must ensure that audit information is archived for six (6) years to enable the recreati is stored.	
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati s stored. References: IRS-1075: 5.6.3.3#5.2	on of computer-related accesses to both the operating syste Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU-	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati s stored. References: IRS-1075: 5.6.3.3#5.2	· · · · · · · · · · · · · · · · · · ·
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective	tit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati s stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1	Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensure	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati s stored. References: IRS-1075: 5.6.3.3#5.2	Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensur- wherever PII is stored.	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati is stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related ac	Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensure wherever PII is stored. Assessment Methods And Object	tit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreation is stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related actions S	Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensure wherever PII is stored. Assessment Methods And Object Examine: PII audit information is re	tit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati s stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related access to both the operation system tained for (6) six years to enable recreation of computer related access to both the operation system	Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensure wherever PII is stored. Assessment Methods And Object Examine: PII audit information is re AU-11(PII-3) – Enhancement (High	tit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati s stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related access to both the operation system tained for (6) six years to enable recreation of computer related access to both the operation system	Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensure wherever PII is stored. Assessment Methods And Object Examine: PII audit information is re AU-11(PII-3) – Enhancement (High Control	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati is stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related access to both the operation system stained for (6) six years to enable recreation of computer related access to both the operation system)	Related Controls: ccesses to both the operation system and the application m and the application wherever PII is stored.
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensure wherever PII is stored. Assessment Methods And Object Examine: PII audit information is re AU-11(PII-3) – Enhancement (High Control For PII, inspection reports, including	<pre>dit records are retained or a control schedule indicates (5) five years or longer.) organizations must ensure that audit information is archived for six (6) years to enable the recreati is stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related access to both the operation system s tained for (6) six years to enable recreation of computer related access to both the operation system) a record of corrective actions, shall be retained by the organization for a minimum of three (3) years</pre>	Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensure wherever PII is stored. Assessment Methods And Object Examine: PII audit information is re AU-11(PII-3) – Enhancement (High Control For PII, inspection reports, including Applicability: All	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati is stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related access to both the operation system tained for (6) six years to enable recreation of computer related access to both the operation system a record of corrective actions, shall be retained by the organization for a minimum of three (3) year References: IRS-1075: 6.3.5#3	Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensur- wherever PII is stored. Assessment Methods And Object Examine: PII audit information is re AU-11(PII-3) – Enhancement (High Control For PII, inspection reports, including Applicability: All ASSESSMENT PROCEDURE: AU-	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati is stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related access to both the operation system tained for (6) six years to enable recreation of computer related access to both the operation system a record of corrective actions, shall be retained by the organization for a minimum of three (3) year References: IRS-1075: 6.3.5#3	Related Controls: ccesses to both the operation system and the application m and the application wherever PII is stored. ars from the date the inspection was completed.
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensur- wherever PII is stored. Assessment Methods And Object Examine: PII audit information is re AU-11(PII-3) – Enhancement (High Control For PII, inspection reports, including Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreati is stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related access tained for (6) six years to enable recreation of computer related access to both the operation system () a record of corrective actions, shall be retained by the organization for a minimum of three (3) yea References: IRS-1075: 6.3.5#3 11(PII-3).1	Related Controls: cccesses to both the operation system and the application m and the application wherever PII is stored. ars from the date the inspection was completed. Related Controls:
Examine: PII disclosure/access aud AU-11(PII-2) – Enhancement (High Control To support the audit of activities, all and to the application wherever PII Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if the organization ensur- wherever PII is stored. Assessment Methods And Object Examine: PII audit information is re AU-11(PII-3) – Enhancement (High Control For PII, inspection reports, including Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective	dit records are retained or a control schedule indicates (5) five years or longer. organizations must ensure that audit information is archived for six (6) years to enable the recreation is stored. References: IRS-1075: 5.6.3.3#5.2 11(PII-2).1 es that audit information is archived for six (6) years to enable the recreation of computer related access to both the operation system a record of corrective actions, shall be retained by the organization for a minimum of three (3) years a record of corrective actions, shall be retained by the organization for a minimum of three (3) years a record of corrective actions, shall be retained by the organization for a minimum of three (3) years a record of corrective actions, shall be retained by the organization for a minimum of three (3) years a record of corrective actions, shall be retained by the organization for a minimum of three (3) years b respection reports include a record of corrective actions, which is retained for a minimum of three (3)	Related Controls: cccesses to both the operation system and the application m and the application wherever PII is stored. ars from the date the inspection was completed. Related Controls:

Certification, Accreditation, and Security Assessments (CA) - Management

CA-1 – Certification, Accreditation, and Security Assessments Policies and Procedures (High)

Control

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the Business Owner and accredited by the CMS CIO or his/her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the confidentiality, integrity, and availability (CIA) of CMS information and information systems. All C&A and security assessment activities shall be conducted in accordance with current CMS Procedures.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs, MAs, and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and/or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.4.6, Security Accreditation (CA-6).

If the CMS CIO or his/her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his/her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his/her designated representatives.

As part of the system certification and accreditation (C&A), an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, IS Risk Assessment (RA), System Security Plan (SSP), independent system tests and evaluations, the Business Owner and System Developer / Maintainer shall certify that the system meets the security requirements to the extent necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CMS CIO or the Designated Accrediting Authority (DAA).

Guidance

The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security control assessments. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: CA-1; FISCAM: TSP-5.1.2; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075:	Related Controls: CA-6
	5.6.1.4#1.1-2; NIST 800-53/53A: CA-1; PISP: 4.4.1	

ASSESSMENT PROCEDURE: CA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security assessment and certification and accreditation policies and procedures;

(ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review policy and procedures; and

(iv) the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.

Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.

ASSESSMENT PROCEDURE: CA-1.2

Assessment Objective

Determine if:

(i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records. **Interview:** Organizational personnel with security assessment and certification and accreditation responsibilities.

CA-2 – Security Assessments (High)

Control

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application, and comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Routine assessments shall be conducted every 365 days, in accordance with NIST SP 800-53 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information system.

OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST SP 800-53 A provides guidance on security control assessments to include reuse of existing assessment results.

Applicability: All	References: ARS: CA-2; FISCAM: TSP-5.1.1; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1; NIST 800-53/53A: CA-2; PISP: 4.4.2	Related Controls: CA-4, CA-6, CA-7, CA-7(1), SA-11, SI-2
ASSESSMENT PROCEDURE: CA-2.1		

Assessment Objective

Determine if:

(i) the information system is in the inventory of major information systems; and

(ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security assessment policy; procedures addressing security assessments; information system security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records.

CA-3 – Information System Connections (High)

Control

Management shall authorize in writing through the use of system connection agreements all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system connections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

Guidance

Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST SP 800-47 provides guidance on connecting information systems.

Applicability: All	References: ARS: CA-3; HSPD 7: F(19); NIST 800-53/53A: CA-3; PISP: 4.4.3	Related Controls: SA-9, SC-7
ASSESSMENT PROCEDURE: CA-3.1	•	

Assessment Objective

Determine if:

(i) the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary);

(ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements;

(iii) the organization monitors/controls the system interconnections on an ongoing basis; and

(iv) information system connection agreements are consistent with NIST SP 800-47.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records.

Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements.

CA-3(CMS-1) – Enhancement (High)

Control

 Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

 Applicability: All
 References: ARS: CA-3(CMS-1); FISCAM: TAC-2.1.3; HSPD 7: F(19)
 Related Controls:

ASSESSMENT PROCEDURE: CA-3(CMS-1).1

Assessment Objective

Determine if the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

CA-4 – Security Certification (High)

Control

Business owners shall conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification process shall be integrated into and span across the SDLC. In addition, the Business Owner shall review the certification documentation every 365 days, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his/her designated representative.

Guidance

A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST SP 800-53 A provides guidance on security certification.

Applicability: All	References: ARS: CA-4; FISCAM: TSS-2.2.4; HSPD 7: F(19); IRS-1075: 6.3#1.1-2; NIST 800-	Related Controls: CA-2, CA-6, CA-7, SA-
	53/53A: CA-4; PISP: 4.4.4	11, SI-2

ASSESSMENT PROCEDURE: CA-4.1

Assessment Objective

Determine if:

(i) the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and

(ii) the organization employs a security certification process in accordance with OMB policy and NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.

Interview: Organizational personnel with security certification responsibilities.

CA-4(1) – Enhancement (High)

Control

Employ an independent certification agent or certification team to conduct an assessment of the information system security controls.

Guidance

An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization had owns the information system or authorizing official, independence in the certification process can be accomplished by individuals that are in the developmental, operational, and/or management chain of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances descr

Applicability: All	References: ARS: CA-4(1); HSPD 7: F(19); NIST 800-53/53A: CA-4(1)	Related Controls: AC-9
ASSESSMENT PROCEDURE: CA-4(1).1		

Assessment Objective

Determine if the organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; security accreditation package (including information system security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.

CA-4(CMS-1) – Enhancement (High)

Control

Document the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures.

Applicability: All	References: ARS: CA-4(CMS-1); HSPD 7: F(19), G(24)	Related Controls:
ASSESSMENT PROCEDURE: CA-4(CMS-1).1		

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.

Interview: Organizational personnel with security certification responsibilities to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.

CA-5 – Plan of Action and Milestones (POA&M) (High)

Control

A POA&M shall be developed, implemented, and updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M shall document the planned, implemented, and evaluated corrective actions to repair deficiencies discovered during the security control assessment, and to reduce or eliminate any known vulnerability in the information system.

Personnel shall be designated to assign, track, and update risk mitigation efforts. Designated personnel shall define and authorize corrective action plans, and monitor corrective action progress.

Guidance

The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems. NIST SP 800-30 provides guidance on risk mitigation.

Applicability: All	References: ARS: CA-5; FISCAM: TSP-5.2; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4; NIST 80 53/53A: CA-5; PISP: 4.4.5	0- Related Controls: CA-7
ASSESSMENT PROCEDURE: CA-5.1	55/55A. CA-5, FISF. 4.4.5	
Assessment Objective		
Determine if:		
(i) the organization develops and updates	at the organization-defined frequency, a plan of action and milestones for the information system; and	
(ii) the plan of action and milestones docur	nents the planned, implemented, and evaluated remedial actions by the organization to correct any deficien	cies noted during the assessment of the securit
controls and to reduce or eliminate known	rulnerabilities in the information system.	
Assessment Methods And Objects		
	plicy; procedures addressing plan of action and milestones; information system security plan; security asses	ssment plan; security assessment report;
2 T	nilestones; other relevant documents or records.	
CA-5(0) – Enhancement (High)	lan of action and milestones development and implementation responsibilities.	
() (3)		
Control	ilestence (DOA 8NA) for any descented information contains accurity finding within thirty (20) down of the fin	
Develop and submit a plan of action and m	ilestones (POA&M) for any documented information system security finding within thirty (30) days of the fina). Update the POA&M monthly until all the findings are resolved.	al results for every internal / external audit /
Applicability: All	References: ARS: CA-5(0); HSPD 7: F(19), G(24); NIST 800-53/53A: CA-5; PISP: 4.4.5	Related Controls:
ASSESSMENT PROCEDURE: CA-5(0).1		
Assessment Objective		
•	quirements as specified in the baseline control and the specific CMS requirements as prescribed in this amp	lifving enhancement to the baseline control
Assessment Methods And Objects		singing enhancement to the baseline control.
	blicy and procedures; information system security plan (for organization-defined frequency of plan of action	and milestones undates); security assessmen
plan: security assessment report: assessm	ent evidence; plan of action and milestones; other relevant documents or records.	and milestones updates), security assessment
	lan of action and milestones development and implementation responsibilities.	
CA-6 – Security Accreditation (High		
Control		
Explicit authorization to operate the inform	ation system shall be received from the CMS CIO or his/her designated representative prior to the system b	eing placed into operations. If the authorization
	authorization shall be granted based on the designated security category of the information system. An exp	
	the authorizing official. Re-authorization shall be obtained prior to continued operation:	
4.4.6.1. At least every three (3) years;		
4.4.6.2. When substantial changes are ma		
	sult in the need to process data of a higher sensitivity;	
4.4.6.4. When changes occur to authorizin	g legislation or federal requirements; ecurity violation which raises questions about the validity of an earlier certification; and	
4.4.6.6. Prior to expiration of a previous ac		
Guidance		
	nes policy for security accreditations of federal information systems. The organization assesses the security	controls employed within the information
	y accreditation. Security assessments conducted in support of security accreditations are called security ce	
	Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of	
	tation package (i.e., the system security plan, the security assessment report, and the plan of action and mi	
	ormation system owner with an up-to-date status of the security state of the information system. To reduce	
reaccreditation process, the authorizing of	icial uses the results of the ongoing continuous monitoring process to the maximum extent possible as the b	basis for rendering a reaccreditation decision.
NIST SP 800-37 provides guidance on the	security certification and accreditation of information systems.	- -
Applicability: All	References: ARS: CA-6; FISCAM: TSP-5.1.3, TSP-5.2; HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6	Related Controls: CA-1, CA-2, CA-4, CA
ASSESSMENT PROCEDURE: CA-6.1		
ASSESSMENT PROCEDURE: CA-6.1		

(i) the organization authorizes (i.e three (3) years;	., accredits) the information system f	or processing before operations and updates the authorization in	n accordance with or	rganization-defined frequency, at least ever
	signs and approves the security accr	editation:		
		consistent with NIST SP 800-37; and		
		ant change to the information system.		
Assessment Methods And Obje				
		g security accreditation; NIST SP 800-37; security accreditation r	package (including i	nformation system security plan: security
		nent); other relevant documents or records.	1	
Interview: Organizational person	nel with security accreditation respon	sibilities.		
CA-6(0) – Enhancement (High)				
Control				
Information systems can only be	accredited for a maximum period of t	hree (3) years, after which the information system must be re-acc	credited.	
Applicability: All	References: ARS: C	CA-6(0); HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6		Related Controls:
ASSESSMENT PROCEDURE: C	4-6(0).1			
Assessment Objective				
Determine if the organization me	ts the requirements as specified in the	ne baseline control and the specific CMS requirements as prescr	ribed in this amplifyir	ng enhancement to the baseline control.
Assessment Methods And Obje	ts			-
		g security accreditation; NIST SP 800-37; security accreditation p	package (including i	nformation system security plan; security
assessment report; plan of action	and milestones; authorization staten	nent); other relevant documents or records.		
Interview: Organizational person	nel with security accreditation respor	sibilities.		
CA-7 – Continuous Monitorir	g (High)			
Control				
Security controls in CMS information	ion systems shall be monitored on a	n on-going basis. Selection criteria for control monitoring shall be	e established and a	subset of the security controls employed
	e selected for continuous monitoring			
Guidance				
Continuous monitoring activities i	clude configuration management ar	d control of information system components, security impact ana	alyses of changes to	the system, ongoing assessment of
security controls, and status repo	ting. The organization assesses all s	security controls in an information system during the initial securit	ity accreditation. Sub	osequent to the initial accreditation and in
		e controls annually during continuous monitoring. The selection		
		cific security controls selected and employed by the organization		
		in determining the effectiveness of the security controls in the in		
		loyed within the information system for assessment. The organiz		
		re volatile or critical to protecting the information system are asse		
assessment requirement (see CA		ne organization can use the current year's assessment results ob	stained during contin	nuous monitoring to meet the annual FISM
		es required in monitoring configuration changes to the informatior	n system An effecti	ve continuous monitoring program results i
ongoing updates to the informatic	n system security plan the security ;	assessment report, and the plan of action and milestones—the th	hree principle docum	pents in the security accreditation package
		itly reduces the level of effort required for the reaccreditation of the		
		nce on the assessment of security controls.		
Applicability: All		CA-7; HSPD 7: F(19); NIST 800-53/53A: CA-7; PISP: 4.4.7		Related Controls: CA-2, CA-4, CA-5, CA-
-				6, CM-4, SI-2
ASSESSMENT PROCEDURE: C	4-7.1			
Assessment Objective				
Determine if:				
(i) the organization monitors the s	ecurity controls in the information sys			
(ii) the organization employs a se	curity control monitoring process con	sistent with NIST SP 800-37 and 800-53A.		
Accordment Methods And Obio	ato .			

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

Interview: Organizational personnel with cont	inuous monitoring responsibilities.		
ASSESSMENT PROCEDURE: CA-7.2			
Assessment Objective			
Determine if:			
	analyses on changes to the information system		
	nanges to or deficiencies in the security control		
	information system security plan and plan of a	action and milestones, as appropriate, b	based on the activities associated with continuous monitoring of the
security controls.			
Assessment Methods And Objects			
plan of action and milestones; information sys	tem monitoring records; security impact analys		Ils; information system security plan; security assessment report; nents or records.
Interview: Organizational personnel with cont	inuous monitoring responsibilities.		
CA-7(1) – Enhancement (High)			
Control			
The use of independent certification agents or satisfy ST&E requirements.	teams is not required but, if used by the organ	nization to monitor the security controls	in the information system on an on-going basis, this can be used to
Guidance			
	e value of the ongoing assessment of security e information system's three-year accreditation		ng process by requiring an independent certification agent or team
Applicability: All	References: ARS: CA-7(1); HSPD 7: F(19); NIST 800-53/53A: CA-7(1)	Related Controls: AC-9, CA-2
ASSESSMENT PROCEDURE: CA-7(1).1			
plan of action and milestones; information sys Interview: Organizational personnel with con	tem monitoring records; security impact analys		ls; information system security plan; security assessment report; nents or records.(Optional)
CA-7(CMS-1) – Enhancement (High)			
Control			
Continuous monitoring activities include:			
(a) Configuration management;			
 (b) Control of information system components (c) Security impact analyses of changes to the 			
(d) On-going assessment of security controls;			
(e) Status reporting.			
Applicability: All	References: ARS: CA-7(CMS-1); HSPD 7	′: F(19)	Related Controls:
ASSESSMENT PROCEDURE: CA-7(CMS-1		\$ <i>L</i>	·
Assessment Objective	<u>/</u>		
Determine if:			
	rols in the information system on an ongoing ba	asis: and	
	I monitoring process consistent with NIST SP 8		
Assessment Methods And Objects	51		
-	v: procedures addressing continuous monitori	ng of information system security control	ls; NIST SP 800-37 and 800-53A; information system security
plan; security assessment report; plan of action continuous monitoring activities include: (a) Configuration management;	on and milestones; information system monitori	ing records; security impact analyses; si	tatus reports; other relevant documents or records to determine
(b) Control of information system components(c) Security impact analyses of changes to the			

(d) On-going assessment of security controls; and

(e) Status reporting.

Interview: Organizational personnel with continuous monitoring responsibilities to determine continuous monitoring activities include:

(a) Configuration management;

(b) Control of information system components;

(c) Security impact analyses of changes to the system;

(d) On-going assessment of security controls; and

(e) Status reporting.

Configuration Management (CM) – Operational

CM-1 – Configuration Management Policy and Procedures (High)

Control

A CM process that includes the approval, testing, implementation, and documentation of changes shall be developed, documented, and implemented effectively to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with the organization's information technology architecture plans. Formally documented CM roles, responsibilities, procedures, and documentation shall be in place.

Guidance

The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: CM-1; FISCAM: TCC-2.1.9, TCC-3.2.1, TCC-3.2.2, TCC-3.3.1, TSS-3.1.1, TSS-	Related Controls:
	3.1.2, TSS-3.1.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-1; PISP: 4.5.1	

ASSESSMENT PROCEDURE: CM-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents configuration management policy and procedures;

(ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review configuration management policy and procedures; and

(iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.

Interview: Organizational personnel with configuration management and control responsibilities.

ASSESSMENT PROCEDURE: CM-1.2

Assessment Objective

Determine if:

(i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.

Interview: Organizational personnel with configuration management and control responsibilities.

CM-2 – Baseline Configuration (High)

Control

A baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system shall be developed and documented. Procedures shall be developed, documented, and implemented effectively to maintain the baseline configuration. The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture.

Guidance

This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture.

Applicability: All	References: ARS: CM-2; HIPAA: 164.310(b); NIST 800-53/53A: CM-2; PISP: 4.5.2	Related Controls: CM-6, CM-8
ASSESSMENT PROCEDURE: CM-2.1		
Assessment Objective		

Assessment Objective

Determine if:

(i) the organization develops, documents, and maintains a baseline configuration of the information system;

(ii) the baseline configuration shows relationships among information system components and is consistent with the Federal Enterprise Architectu	
(iii) the baseline configuration provides the organization with a well-defined and documented specification to which the information system is built;	and
(iv) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.	
Assessment Methods And Objects Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Arcl	aitecture documentation: information system design
documentation; information system architecture and configuration documentation; other relevant documents or records.	inecture documentation, information system design
CM-2(1) – Enhancement (High)	
Control	
Update the baseline configuration of the information system as an integral part of information system component installations.	
Applicability: All References: ARS: CM-2(1); NIST 800-53/53A: CM-2(1)	Related Controls:
ASSESSMENT PROCEDURE: CM-2(1).1	
Assessment Objective	
Determine if:	
(i) the organization identifies the frequency of updates to the baseline configuration and instances that trigger configuration updates; and	
(ii) the organization updates the baseline configuration of the information system as an integral part of information system component installations	
Assessment Methods And Objects	
Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; information system arc	hitecture and configuration documentation; other
relevant documents or records.	
CM-2(2) – Enhancement (High)	
Control	
Employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information syst	
Applicability: All References: ARS: CM-2(2); NIST 800-53/53A: CM-2(2)	Related Controls:
ASSESSMENT PROCEDURE: CM-2(2).1	
Assessment Objective	
Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline confi	guration of the information system.
Assessment Methods And Objects	
Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; information system des and configuration documentation; other relevant documents or records.	ign documentation; information system architecture
Test: Automated mechanisms implementing baseline configuration maintenance.	
CM-2(CMS-1) – Enhancement (High)	
Control	
Review and, if necessary, update the baseline configuration and any other system-related operations or security documentation at least once eve	ry year, and while planning major system changes /
upgrades.	y year, and while planning major system changes /
Applicability: All References: ARS: CM-2(CMS-1); FISCAM: TSS-3.2.6	Related Controls:
ASSESSMENT PROCEDURE: CM-2(CMS-1).1	· ·
Assessment Objective	
Determine if the organization develops, documents, and maintains a baseline configuration of the information system.	
Assessment Methods And Objects	
Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Arcl	nitecture documentation; information system design
documentation; information system architecture and configuration documentation; other relevant documents or records to determine the baseline	
operations or security documentation are reviewed and updated at least once every year, and while planning major system changes / upgrades.	
Interview: Organizational personnel with configuration management responsibilities to determine the baseline configuration and any other system reviewed and updated at least once every year, and while planning major system changes / upgrades.	related operations or security documentation are
CM-2(CMS-2) – Enhancement (High)	
Control Maintain on undeted list of the information system's operations and acquirity desumentation	
Maintain an updated list of the information system's operations and security documentation.	

Applicability: All	References: ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6	Related Controls:
ASSESSMENT PROCEDURE: CM-2(CMS		
Assessment Objective		
	seline configuration of the information system as an integral part of information system component installati	ions
Assessment Methods And Objects		
-	; procedures addressing the baseline configuration of the information system; Federal Enterprise Architectu	ire documentation: information system design
	ure and configuration documentation; other relevant documents or records to determine an updated list of the	
J	nfiguration management responsibilities to determine an updated list of the information system's operations	and security documentation is maintained.
CM-3 – Configuration Change Contro		
Control	. (
	e and supporting procedures shall be developed, documented, and implemented effectively to control chan	ges to the information system. Change
request forms shall be used to document re-	Juests with related approvals. Change requests shall be approved by the Business Owner, or his/her desig d to, the system maintainer and information system support staff.	
	for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers of security. Test results shall be documented and appropriate responsive actions shall be taken based on the	
	n system shall be documented and approved by appropriate organization officials, either prior to the change tely and approved, and responsible personnel shall be notified for security analysis and follow-up.	e or after the fact. Emergency changes to the
Guidance		
involves the systematic proposal justification		
change control includes changes to the con configuration change control process, includ security analysis of the change. The organiz	n, implementation, test/evaluation, review, and disposition of changes to the information system, including u iguration settings for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system.	nization includes emergency changes in the n system include successful results from the
change control includes changes to the con configuration change control process, include	 ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 	nization includes emergency changes in the
change control includes changes to the con configuration change control process, includ security analysis of the change. The organiz	guration settings for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-	nization includes emergency changes in the n system include successful results from the
change control includes changes to the con- configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1	 ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 	nization includes emergency changes in the n system include successful results from the
change control includes changes to the control figuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective	 ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 	nization includes emergency changes in the n system include successful results from the
change control includes changes to the control figuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if:	 ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the informatio ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 	nization includes emergency changes in the n system include successful results from the
change control includes changes to the con- configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a	ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the informatio ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3	nization includes emergency changes in the n system include successful results from the
change control includes changes to the con- configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of	ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the informatio ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; hanges to the information system using an organizationally approved process;	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the con- configuration change control process, includes security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization includes emergency cha	ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the informatio ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; shanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws	nization includes emergency changes in the in system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the com configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization includes emergency cha (iv) the organization audits activities associa	ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the informatio ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; hanges to the information system using an organizationally approved process;	nization includes emergency changes in the in system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the con- configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization includes emergency cha (iv) the organization audits activities associa Assessment Methods And Objects Examine: Configuration management policy	ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the information ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; shanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the con- configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization manages configuration of (iii) the organization audits activities associa Assessment Methods And Objects Examine: Configuration management policy control records; information system audit rea	ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the information ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; shanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the con- configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization includes emergency ch- (iv) the organization audits activities associa Assessment Methods And Objects Examine: Configuration management policy control records; information system audit ref	ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the information ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; shanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the cont configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization includes emergency cha (iii) the organization audits activities associa Assessment Methods And Objects Examine: Configuration management policy control records; information system audit ref CM-3(1) – Enhancement (High)	ing changes resulting for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the information ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; shanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the com configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization manages configuration of (iii) the organization auditor activities associa Assessment Methods And Objects Examine: Configuration management policy control records; information system audit ref CM-3(1) – Enhancement (High) Control Employ automated mechanisms to:	Iguration settings for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system. References: RRS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; hanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a ords; other relevant documents or records.	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the con- configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration o (iii) the organization includes emergency ch- (iv) the organization audits activities associa Assessment Methods And Objects Examine: Configuration management policy control records; information system audit ref CM-3(1) – Enhancement (High)	Iguration settings for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system. References: RRS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; hanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a ords; other relevant documents or records.	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the com configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization manages configuration of (iii) the organization includes emergency cha (iv) the organization audits activities associa Assessment Methods And Objects Examine: Configuration management policy control records; information system audit rec CM-3(1) – Enhancement (High) Control Employ automated mechanisms to: (a) Document proposed changes to the information of the system of the information of the system of the information	iguration settings for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; hanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a ords; other relevant documents or records.	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the com configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization manages configuration of (iii) the organization includes emergency cha (iv) the organization audits activities associa Assessment Methods And Objects Examine: Configuration management policy control records; information system audit rea CM-3(1) – Enhancement (High) Control Employ automated mechanisms to: (a) Document proposed changes to the info (b) Notify appropriate approval authorities,	iguration settings for information technology products (e.g., operating systems, firewalls, routers). The organing changes resulting from the remediation of flaws. The approvals to implement a change to the information audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 Ind controls changes to the information system; hanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a ords; other relevant documents or records.	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2
change control includes changes to the com configuration change control process, include security analysis of the change. The organiz Applicability: All ASSESSMENT PROCEDURE: CM-3.1 Assessment Objective Determine if: (i) the organization authorizes, documents, a (ii) the organization manages configuration of (iii) the organization manages configuration of (iii) the organization includes emergency cha (iv) the organization audits activities associa Assessment Methods And Objects Examine: Configuration management policy control records; information system audit ref CM-3(1) – Enhancement (High) Control Employ automated mechanisms to: (a) Document proposed changes to the info (b) Notify appropriate approval authorities, (c) Identify approvals that have not been ref	iguration settings for information technology products (e.g., operating systems, firewalls, routers). The organ ing changes resulting from the remediation of flaws. The approvals to implement a change to the information ation audits activities associated with configuration changes to the information system. References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.4, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3 and controls changes to the information system; thanges to the information system using an organizationally approved process; inges in the configuration change control process, including changes resulting from the remediation of flaws ted with configuration changes to the information system. ; procedures addressing information system configuration change control; information system architecture a ords; other relevant documents or records. mation system, eived in a timely manner, are received, and	nization includes emergency changes in the n system include successful results from the Related Controls: CM-4, CM-6, SI-2

ASSESSMENT PROCEDURE: CM-3(1).1

Assessment Objective

Determine if:

(i) the organization employs automated mechanisms to document proposed changes to the information system;

(ii) the organization employs automated mechanisms to notify appropriate approval authorities;

(iii) the organization employs automated mechanisms to highlight approvals that have not been received in a timely manner;

(iv) the organization employs automated mechanisms to inhibit change until necessary approvals are received; and

(v) the organization employs automated mechanisms to document completed changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records. Test: Automated mechanisms implementing configuration change control.

Test: Automated mechanisms implementing configuration cha

CM-3(FIS-1) – Enhancement (High)

Control

Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.

Applicability: All	References: FISCAM: TCC-2.1.11	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-1).1		

Assessment Objective

Determine if the organization reviews production program changes for access and change control compliance.

Assessment Methods And Objects

Examine: Documentation of management or security administrator reviews.

Examine: Pertinent policies and procedures.

Interview: Information system management or security administrators.

CM-3(FIS-2) – Enhancement (High)

Control

Migration of tested and approved system software to production use is performed by an independent library control group.

Applicability: All	References: FISCAM: TSS-3.2.2	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-2).1		

Assessment Objective

Determine if the organizational independent library control group migrates tested and approved software into production.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation for some system software migrations.

Interview: Management, systems programmers, and library control personnel, and determine who migrates approved system software to production libraries.

CM-3(FIS-3) – Enhancement (High)

Control

Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.

Applicability: All	References: FISCAM: TSS-3.2.1	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-3).1		

Assessment Objective

Determine if the organization provides advance schedules to system users which minimize system software installation impacts.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Recent installations and determine whether scheduling and advance notification did occur.

Interview: Management and systems programmers about scheduling and giving advance notices when system software is installed.

CM-3(FIS-4) – Enhancement (High)	
Control	
Outdated versions of system software are removed from production libraries.	
Applicability: All References: FISCAM: TSS-3.2.3	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-4).1	
Assessment Objective	
Determine if the organization removes outdated versions of system software from the production libraries.	
Assessment Methods And Objects	
Examine: Pertinent policies and procedures.	
Examine: Supporting documentation for the removal of outdated versions from production libraries.	no duction librarian
Interview: Management, systems programmers, and library control personnel, and determine whether outdated versions are removed from pro-	roduction libraries.
CM-4 – Monitoring Configuration Changes (High)	
Control	
Mechanisms to monitor change activity shall be in place and supporting procedures shall be developed, documented, and implemented effective by privileged users. Security impact analyses shall be conducted after system changes are made to determine the IS-related effects of the character to the information system changes are made to determine the IS-related effects of the character to the information system changes are made to determine the IS-related effects of the character to the information system changes are made to determine the IS-related effects of the character to the information system changes are made to determine the IS-related effects of the character to the information system changes are made to determine the IS-related effects of the character to the information system.	
to the information system shall be audited. Guidance	
	potential acquirity impacts. After the information system
Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning	
with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important	
security controls in the information system.	
Applicability: All References: ARS: CM-4; FISCAM: TCC-2.1.11, TCC-2.2.2, TCC-2.3.1, TCC-3.1, TSS-3.1.4; 800-53/53A: CM-4; PISP: 4.5.4 800-53/53A: CM-4; PISP: 4.5.4	I; NIST Related Controls: CA-7, CM-3
ASSESSMENT PROCEDURE: CM-4.1	
Assessment Objective	
Determine if:	
(i) the organization identifies the types of information system changes to be monitored;	
(ii) the organization monitors changes to the information system; and	
(iii) the organization conducts security impact analyses to assess the effects of the information system changes.	
Assessment Methods And Objects	
Examine: Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; inform	nation system architecture and configuration
documentation; change control records; information system audit records; other relevant documents or records.	
CM-4(CMS-1) – Enhancement (High)	
Control	
When changes to the system occur, record the installation of information system components in the appropriate system documentation resource	
Applicability: All References: ARS: CM-4(CMS-1); FISCAM: TCC-2.1.10, TCC-2.2.2, TCC-2.3.1, TCC-3.1, TS	SS-3.1.4 Related Controls:
ASSESSMENT PROCEDURE: CM-4(CMS-1).1	
Assessment Objective	
Determine if:	
(i) the organization identifies the types of information system changes to be monitored;	
(ii) the organization monitors changes to the information system; and(iii) the organization conducts security impact analyses to assess the effects of the information system changes.	
Assessment Methods And Objects	
Examine: Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; inform	nation system architecture and configuration
documentation; change control records; information system audit records; other relevant documents or records to determine that when change system components is recorded in the appropriate system documentation resource(s).	es to the system occur, the installation of information
Interview: Organizational personnel with information system monitoring responsibilities to determine that when changes to the system occur,	, the installation of information system components is

CM-4(FIS-1) – Enhancement (High) Control		
Control		
Library management software is used to: (1) n control concurrent updates.	maintain program version numbers, (2) maintain creation/date information for prod	luction modules, (3) maintain copies of previous versions, and (4)
Applicability: All	References: FISCAM: TCC-3.1	Related Controls:
ASSESSMENT PROCEDURE: CM-4(FIS-1).	.1	
Assessment Objective		
Determine if the organization uses library man previous versions, and (4) control concurrent	nagement software to: (1) maintain program version numbers, (2) maintain creatio updates.	m/date information for production modules, (3) maintain copies of
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
	in the library and assess compliance with prescribed procedures.	
Interview: Personnel responsible for library co		
Test: Verify how many prior versions of softwa	vare modules are maintained.	
CM-4(FIS-2) – Enhancement (High)		
Control		
	maintained and compared to ensure that only approved changes are made.	
Applicability: All	References: FISCAM: TCC-3.3.2	Related Controls:
ASSESSMENT PROCEDURE: CM-4(FIS-2). Assessment Objective	.1	
Assessment Methods And Objects Examine: For a selection of program changes Examine: Pertinent policies and procedures. Interview: Application programmers, if availab	s, examine related documentation to verify that before and after images were com ble.	npared.
Examine: For a selection of program changes Examine: Pertinent policies and procedures.	ble.	ipared.
Examine: For a selection of program changes Examine: Pertinent policies and procedures. Interview: Application programmers, if availab	ble.	ipared.
Examine: For a selection of program changes Examine: Pertinent policies and procedures. Interview: Application programmers, if availat CM-5 – Access Restrictions for Chang Control Access control change mechanisms shall be i	ble.	ented effectively to approve individual access privileges and to enforce
Examine: For a selection of program changes Examine: Pertinent policies and procedures. Interview: Application programmers, if availat CM-5 – Access Restrictions for Chang Control Access control change mechanisms shall be i	ble. ge (High) in place and supporting procedures shall be developed, documented, and impleme	ented effectively to approve individual access privileges and to enforce
Examine: For a selection of program changes Examine: Pertinent policies and procedures. Interview: Application programmers, if availat CM-5 – Access Restrictions for Chang Control Access control change mechanisms shall be i physical and logical access restrictions associ Guidance Planned or unplanned changes to the hardwa	ble. ge (High) in place and supporting procedures shall be developed, documented, and implementated with changes to the information system. Records reflecting all such changes are, software, and/or firmware components of the information system can have sign cess to information system components for purposes of initiating changes, includir	ented effectively to approve individual access privileges and to enforce s shall be generated, reviewed, and retained. nificant effects on the overall security of the system. Accordingly, only ng upgrades, and modifications.
Examine: For a selection of program changes Examine: Pertinent policies and procedures. Interview: Application programmers, if availat CM-5 – Access Restrictions for Chang Control Access control change mechanisms shall be i physical and logical access restrictions associ Guidance Planned or unplanned changes to the hardwa	ble. ge (High) in place and supporting procedures shall be developed, documented, and implement ciated with changes to the information system. Records reflecting all such changes are, software, and/or firmware components of the information system can have sig	ented effectively to approve individual access privileges and to enforce s shall be generated, reviewed, and retained. nificant effects on the overall security of the system. Accordingly, only ng upgrades, and modifications.
Examine: For a selection of program changes Examine: Pertinent policies and procedures. Interview: Application programmers, if availat CM-5 – Access Restrictions for Chang Control Access control change mechanisms shall be i physical and logical access restrictions associ Guidance Planned or unplanned changes to the hardwa qualified and authorized individuals obtain acc	ble. ge (High) in place and supporting procedures shall be developed, documented, and implementated with changes to the information system. Records reflecting all such changes are, software, and/or firmware components of the information system can have signed cess to information system components for purposes of initiating changes, includir References: ARS: CM-5; FISCAM: TCC-3.2.3, TCC-3.3.1, TSS-1.2.1, TSS-1	ented effectively to approve individual access privileges and to enforce s shall be generated, reviewed, and retained. nificant effects on the overall security of the system. Accordingly, only ng upgrades, and modifications.
Examine: For a selection of program changes Examine: Pertinent policies and procedures. Interview: Application programmers, if availab CM-5 – Access Restrictions for Chang Control Access control change mechanisms shall be i physical and logical access restrictions associ Guidance Planned or unplanned changes to the hardwa qualified and authorized individuals obtain acc Applicability: All	ble. ge (High) in place and supporting procedures shall be developed, documented, and implementated with changes to the information system. Records reflecting all such changes are, software, and/or firmware components of the information system can have signed cess to information system components for purposes of initiating changes, includir References: ARS: CM-5; FISCAM: TCC-3.2.3, TCC-3.3.1, TSS-1.2.1, TSS-1	ented effectively to approve individual access privileges and to enforce s shall be generated, reviewed, and retained. nificant effects on the overall security of the system. Accordingly, only ng upgrades, and modifications.

CM-5(1) – Enhancement (High)		
Control		
Employ automated mechanisms to enforce acces	ss restrictions and to support auditing of the enforcement actions.	
Applicability: All	References: ARS: CM-5(1); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-5(1)	Related Controls:
ASSESSMENT PROCEDURE: CM-5(1).1		
Assessment Objective		
	I mechanisms to enforce access restrictions and support auditing of the enforcement actions.	
Assessment Methods And Objects		
	cedures addressing access restrictions for changes to the information system; information system des	sign documentation; information system
0	ange control records; information system audit records; other relevant documents or records.	
	ess restrictions for changes to the information system.	
CM-6 – Configuration Settings (High)		
Control		
configuration settings for information technology	d implemented effectively to configure and benchmark information technology products in accordance products employed within the information system shall be established. The security settings of information system operational requirements, documented, and enforced in all components of the information	ation technology products shall be configured
Guidance		
settings in accordance with organizational policie	neters of the information technology products that compose the information system. Organizations more s and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements nfiguration settings for information technology products employed in organizational information system.	for federal information systems. NIST SP 800
Applicability: All	References: ARS: CM-6; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6; PISP: 4.5.6	Related Controls: CM-2, CM-3, CM-8, SI
ASSESSMENT PROCEDURE: CM-6.1		
Assessment Objective		
Determine if:		
(i) the organization establishes mandatory config	uration settings for information technology products employed within the information system;	
(ii) the organization configures the security setting	gs of information technology products to the most restrictive mode consistent with operational requiren	nents;
(iii) the organization documents the configuration	5	
	ettings in all components of the information system.	
Assessment Methods And Objects		
Examine: Configuration management policy; pro SP 800-70: other relevant documents or records.	cedures addressing configuration settings for the information system; information system configuration	n settings and associated documentation; NIS
Test: Information system configuration settings.		
Test: Information system configuration settings. CM-6(1) – Enhancement (High)		
Test: Information system configuration settings. CM-6(1) – Enhancement (High) Control		
Test: Information system configuration settings. CM-6(1) – Enhancement (High) Control Employ automated mechanisms to centrally man	age, apply, and verify configuration settings.	Related Controls:
Test: Information system configuration settings. CM-6(1) – Enhancement (High) Control Employ automated mechanisms to centrally man Applicability: All		Related Controls:
Test: Information system configuration settings. CM-6(1) – Enhancement (High) Control Employ automated mechanisms to centrally man Applicability: All ASSESSMENT PROCEDURE: CM-6(1).1	age, apply, and verify configuration settings.	Related Controls:
Test: Information system configuration settings. CM-6(1) – Enhancement (High) Control Employ automated mechanisms to centrally man Applicability: All ASSESSMENT PROCEDURE: CM-6(1).1 Assessment Objective	age, apply, and verify configuration settings. References: ARS: CM-6(1); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6(1)	Related Controls:
Test: Information system configuration settings. CM-6(1) – Enhancement (High) Control Employ automated mechanisms to centrally man Applicability: All ASSESSMENT PROCEDURE: CM-6(1).1 Assessment Objective Determine if the information system employs automatical	age, apply, and verify configuration settings.	Related Controls:
Test: Information system configuration settings. CM-6(1) – Enhancement (High) Control Employ automated mechanisms to centrally man Applicability: All ASSESSMENT PROCEDURE: CM-6(1).1 Assessment Objective Determine if the information system employs automatication Assessment Methods And Objects	age, apply, and verify configuration settings. References: ARS: CM-6(1); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6(1) omated mechanisms to centrally manage, apply, and verify configuration settings.	
Test: Information system configuration settings. CM-6(1) – Enhancement (High) Control Employ automated mechanisms to centrally man Applicability: All ASSESSMENT PROCEDURE: CM-6(1).1 Assessment Objective Determine if the information system employs automatic Assessment Methods And Objects	age, apply, and verify configuration settings. References: ARS: CM-6(1); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6(1) omated mechanisms to centrally manage, apply, and verify configuration settings. cedures addressing configuration settings for the information system; information system design docu	

CM-6(CMS-1) – Enhancement (High) Control Configure the information system to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality. References: ARS: CM-6(CMS-1); IRS-1075; 5.6.2.3#1 **Related Controls:** Applicability: All ASSESSMENT PROCEDURE: CM-6(CMS-1).1 Assessment Objective Determine if: (i) the organization establishes mandatory configuration settings for information technology products employed within the information system; (ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; and (iii) the organization documents the configuration settings. **Assessment Methods And Objects** Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST SP 800-70: other relevant documents or records to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality. Interview: Organizational personnel with configuration management responsibilities to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality. Test: Information system to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality. CM-7 – Least Functionality (High) Control Information systems shall be configured to provide only essential capabilities. The functions and services provided by CMS information systems shall be reviewed carefully to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol [VoIP], Instant Messaging [IM], File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP], file sharing). The use of those functions, ports, protocols, and/or services shall be prohibited and/or restricted. Guidance Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing). Applicability: All References: ARS: CM-7: IRS-1075: 5.6.2.3#1: NIST 800-53/53A: CM-7: PISP: 4.5.7 **Related Controls:** ASSESSMENT PROCEDURE: CM-7.1 **Assessment Objective** Determine if: (i) the organization identifies prohibited or restricted functions, ports, protocols, and services for the information system; (ii) the organization configures the information system to provide only essential capabilities; and (iii) the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services. Assessment Methods And Objects Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan; information system configuration settings and associated documentation: other relevant documents or records. Test: Information system for disabling or restriction of functions, ports, protocols, and services. CM-7(0) – Enhancement (High) Control Configure the information system specifically to only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system / application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled. Applicability: All References: ARS: CM-7(0); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7; PISP: 4.5.7 **Related Controls:**

ASSESSMENT PROCEDURE: CM-7(0).1					
Assessment Objective					
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.					
Assessment Methods And Objects					
Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan (for list of organization-defined prohibited or restricted functions, ports, protocols, and services for the information system); information system configuration settings and associated documentation; other relevant documents or records.					
Test: Information system configuration settings.					
CM-7(1) – Enhancement (High)					
Control					
Review the information system every 365 days o services.	r on an incremental basis where all parts are addressed within a year, to identify and eliminate unnecess	sary functions, ports, protocols, and/or			
Applicability: All	References: ARS: CM-7(1); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7(1)	Related Controls:			
ASSESSMENT PROCEDURE: CM-7(1).1					
Assessment Objective					
Determine if:					
	nformation system reviews to identify and eliminate unnecessary functions, ports, protocols, and service				
() 0	m to identify and eliminate unnecessary functions, ports, protocols, and/or services in accordance with t	he organizational defined frequency.			
Assessment Methods And Objects					
Examine: Configuration management policy; pro associated documentation; other relevant docum	cedures addressing least functionality in the information system; information system security plan; inforr ents or records.	nation system configuration settings and			
CM-8 – Information System Component	Inventory (High)				
Control					
	d implemented effectively to document and maintain a current inventory of the information system's cons components shall include manufacturer, model / type, serial number, version number, location (i.e., phy				
Guidance					
The organization determines the appropriate level	el of granularity for the information system components included in the inventory that are subject to mana includes any information determined to be necessary by the organization to achieve effective property a				
	ion, system/component owner). The component inventory is consistent with the accreditation boundary				
Applicability: All	References: ARS: CM-8; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8; PISP: 4.5.8	Related Controls: CM-2, CM-6			
ASSESSMENT PROCEDURE: CM-8.1		•			
Assessment Objective					
Determine if:					
(i) the organization develops, documents, and ma	aintains a current inventory of the components of the information system; and				
	nts includes any information determined to be necessary by the organization to achieve effective propert	y accountability.			
Assessment Methods And Objects					
	cedures addressing information system component inventory; information system inventory records; oth	er relevant documents or records.			
CM-8(1) – Enhancement (High)					
Control					
	tory as an integral part of component installations.	1			
Applicability: All	References: ARS: CM-8(1); HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8(1)	Related Controls:			
ASSESSMENT PROCEDURE: CM-8(1).1					
Assessment Objective					
Determine if the organization updates the inventor	bry of information system components as an integral part of component installations.				

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records.

Interview: Organizational personnel with information system installation and inventory responsibilities.

CM-8(2) – Enhancement (High) Control Employ automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. Applicability: All References: ARS: CM-8(2); HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8(2)) Related Controls: ASSESSMENT PROCEDURE: CM-8(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records.

Test: Automated mechanisms implementing information system component inventory management.

Contingency Planning (CP) – Operational

CP-1 – Contingency Planning Policy and Procedures (High)

Control

All major CMS information systems shall be covered by a CP that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

Guidance

The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-34 provides guidance on contingency planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: 1075: 5.6.2.2	4.308(a)(7)(ii)(B); IRS-	Rel	ated Controls:

ASSESSMENT PROCEDURE: CP-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents contingency planning policy and procedures;

(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and

(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

ASSESSMENT PROCEDURE: CP-1.2

Assessment Objective

Determine if:

(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-2 – Contingency Plan (High)

Control

All major CMS information systems shall be covered by a CP, relative to the system security level, providing continuity of support in the event of a disruption of service. A CP for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A CP for the information system shall be consistent with NIST SP 800-34. Designated officials within the organization shall review and approve the CP and distribute copies of the plan to key contingency personnel.

Guidance

Contingency Plans consist of all components listed in the CMS Business Partners system Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.

Applicability: All	References: ARS: CP-2; FISCAM: TSC-1.1, TSC-1.2, TSC-1.3, TSC-2.1.2, TSC-3.1.1, TSC-3.1.2,	Related Controls:
	TSC-3.1.3, TSC-3.1.4, TSC-3.2.3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i);	
	IRS-1075: 5.6.2.2#1.3; NIST 800-53/53A: CP-2; PISP: 4.6.2	

ASSESSMENT PROCEDURE: CP-2.1

Assessment Objective

CMS Core Securit	y Requirements for High	Impact Level Assessments
	y Requirements for High	

(i) the organization develops and documents a contingency plan for the information system;			
(ii) the contingency plan is consistent with NIST SP 800-34;			
(iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure;			
(iv) the contingency plan is reviewed and approved by designated organizational officials; and			
(v) the organization disseminates the contingency plan to key contingency personnel.			
Assessment Methods And Objects			
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; NIST SP 800-34; contingency plan; other relevant documents or records.			
ASSESSMENT PROCEDURE: CP-2.2			
Assessment Objective			
Determine if key contingency personnel and the key operating elements within the organization understand the contingency plan and are ready to implement the plan. Assessment Methods And Objects			
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.			
CP-2(1) – Enhancement (High)			
Control			
Coordinate development of the Contingency Plan (CP) with parties responsible for related plans, such as the Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan (COOP), Business Recovery Plan, and Incident Response Plan.			
Guidance			
Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.			
Applicability: All References: ARS: CP-2(1); FISCAM: TSC-3.1.3; HIPAA: 164.308(a)(7)(ii)(E); HSPD 7: G(22)(i); NIST Related Controls: 800-53/53A: CP-2(1) 800-53/53A: CP-2(1) 800-53/53A: CP-2(1) 800-53/53A: CP-2(1)			
ASSESSMENT PROCEDURE: CP-2(1).1			
Assessment Objective			
Determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery			
Plan, Incident Response Plan, Emergency Action Plan).			
Assessment Methods And Objects			
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records.			
Interview: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas.			
CP-2(2) – Enhancement (High)			
Control			
Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.			
Applicability: All References: ARS: CP-2(2); HSPD 7: G(22)(i); NIST 800-53/53A: CP-2(2) Related Controls:			
ASSESSMENT PROCEDURE: CP-2(2).1			
Assessment Objective			
Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.			
Assessment Methods And Objects			
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or			
records.			
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.			
CP-3 – Contingency Training (High)			
Control			
Operational and support personnel (including managers and users of the information system) shall receive training in contingency operations and understand their contingency roles and responsibilities with respect to the information system. Refresher training shall be provided to all contingency personnel.			
Guidance			
Managers, responsible for contingency operations, and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirmed that appropriate training has been completed.			

be documented and confirmed that appropriate training has been completed.

	References: ARS: CP-3; FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3	Related Controls:			
ASSESSMENT PROCEDURE: CP-3.1					
Assessment Objective					
Determine if:					
	g to personnel with significant contingency roles and responsibilities;				
(ii) the organization records the type of continge					
	(iii) the organization defines frequency of refresher contingency training; and (iv) the organization-defined frequency, at least annually.				
Assessment Methods And Objects	renesher training in accordance with organization-defined nequency, at least annually.				
-	ency plan; procedures addressing contingency training; contingency training curriculum; contingency trair	ing material: information system security			
plan; other relevant documents or records.		ing material, information system security			
	gency planning, plan implementation, and training responsibilities.				
ASSESSMENT PROCEDURE: CP-3.2					
Assessment Objective		1.114			
o , o	esses the procedures and activities necessary to fulfill identified organizational contingency roles and resp	oonsidilities.			
Assessment Methods And Objects					
	ency plan; procedures addressing contingency training; contingency training curriculum; contingency trair	ning material; other relevant documents or			
records. CP-3(0) – Enhancement (High)					
Control					
Provide training every 365 days in contingency	roles and responsibilities.				
Applicability: All	References: ARS: CP-3(0); FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3	Related Controls:			
ASSESSMENT PROCEDURE: CP-3(0).1					
Assessment Objective					
	ments as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ing enhancement to the baseline control.			
Assessment Methods And Objects					
(for organization-defined frequency for refreshe	ency plan; procedures addressing contingency training; contingency training curriculum; contingency trair r contingency training); other relevant documents or records.	ning material; information system security plan			
	gency planning, plan implementation, and training responsibilities.				
CP-3(1) – Enhancement (High)					
Control					
	aining to facilitate effective response by personnel in crisis situations.	1			
Applicability: All	References: ARS: CP-3(1); HSPD 7: G(22)(i); NIST 800-53/53A: CP-3(1)	Related Controls:			
ASSESSMENT PROCEDURE: CP-3(1).1					
Assessment Objective					
Determine if:					
(i) the organization incorporates simulated ever					
	nal personnel to respond as expected to simulated crisis situations.				
Assessment Methods And Objects					
Examine: Contingency planning policy; conting records.	ency plan; procedures addressing contingency training; contingency training curriculum; contingency trair	ing material; other relevant documents or			
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.					
CP-3(2) – Enhancement (High)					
Control					
Employ automated mechanisms to provide thor	bugh and realistic training environments.				

Applicability: All	References: ARS: CP-3(2); HSPD 7: G(22)(i); NIST 800-53/53A: CP-3(2)	Related Controls:
ASSESSMENT PROCEDURE: C		
Assessment Objective		
Determine if:		
	omated mechanisms for contingency training; and	
(ii) the automated mechanisms in	improve the effectiveness of the contingency training.	
Assessment Methods And Obje	ects	
contingency training material; oth	g policy; contingency plan; procedures addressing contingency training; automated mechanisms suppor ther relevant documents or records.(Optional)	rting contingency training; contingency training curriculum;
	onnel with contingency planning, plan implementation, and training responsibilities.(Optional)	
CP-4 – Contingency Plan Te	esting and Exercises (High)	
Control		
effectiveness and readiness to e	cised at least every 365 days using defined tests and exercises, such as the tabletop test in accordance execute the plan. Test / exercise results shall be documented and reviewed by appropriate organization the impact of CP failures and deficiencies.	
Guidance	_ ·	
There are several methods for te rigor of contingency plan testing effects on organizational operation guidance on test, training, and e	esting and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plar ions and assets (e.g., reduction in mission capability) and individuals arising due to contingency operati exercise programs for information technology plans and capabilities.	n testing and/or exercises also include a determination of the
Applicability: All	References: ARS: CP-4; FISCAM: TSC-1.1, TSC-4.1, TSC-4.2.1, TSC-4.2.2; HIPAA	
	164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2; NI CP-4; PISP: 4.6.4	IST 800-53/53A:
ASSESSMENT PROCEDURE: C	CP-4.1	
Assessment Objective		
Determine if:		
0	requency of contingency plan tests and/or exercises;	
() 0	set of contingency plan tests and/or exercises;	
	ises the contingency plan using organization-defined tests/exercises in accordance with organization-de	efined frequency;
	the results of contingency plan testing/exercises; and	
	contingency plan test/exercise results and takes corrective actions.	
Assessment Methods And Obje		
	g policy; contingency plan, procedures addressing contingency plan testing and exercises; information s	system security plan; contingency plan testing and/or exercise
documentation; other relevant do		
ASSESSMENT PROCEDURE: C	JT-4.2	
Assessment Objective	an tao ta da anna an an anna an an tao a tao an	
0,1	an tests/exercises address key aspects of the plan.	
Assessment Methods And Obje		
test results; other relevant docur	g policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency	plan testing and/or exercise documentation; contingency plan
CP-4(0) – Enhancement (High)		
Control	enteble testeductions and factors of tebleton consistence of a section burget of the sector of the s	a detection and a det
	ecutable, tested using a combination of tabletop exercises and operational tests every 365 days, and up	
Applicability: All	References: ARS: CP-4(0); FISCAM: TSC-4.1; HSPD 7: G(22)(i); NIST 800-53/53A: 4.6.4	CP-4; PISP: Related Controls:

ASSESSMENT PROCEDURE: CP-4(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan (for the organization-defined frequency of contingency plan tests and/or exercises and the list of the organization-defined contingency plan tests and/or exercises); contingency plan testing and/or exercise documentation; other relevant documents or records.

CP-4(1) – Enhancement (High)

Control

Coordinate testing and exercising of CP with parties responsible for related plans, such as:

(a) Business Continuity Plan,

(b) Disaster Recovery Plan,

(c) Continuity of Operations Plan,

(d) Business Recovery Plan, and

(e) Incident Response Plan.

Guidance

 Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

 Applicability: All
 References: ARS: CP-4(1); HSPD 7: G(22)(i); NIST 800-53/53A: CP-4(1)
 Related Controls:

ASSESSMENT PROCEDURE: CP-4(1).1

Assessment Objective

Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.

Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities.

CP-4(2) – Enhancement (High)

Control

Test / exercise the CP at the alternate processing site to evaluate the site's capabilities to support contingency operations.

Applicability: All	References: ARS: CP-4(2); HSPD 7: G(22)(i); NIST 800-53/53A: CP-4(2)	Related Controls:

ASSESSMENT PROCEDURE: CP-4(2).1

Assessment Objective

Determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records.

CP-4(3) – Enhancement (High)

Control

Employ automated mechanisms to more thoroughly and effectively test / exercise the CP by providing more complete coverage of contingency issues, selecting more realistic test / exercise scenarios and environments, and more effectively stressing the information system and supported missions.

Applicability: All	References: ARS: CP-4(3); FISCAM: TSC-4.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-4(3)	Related Controls:
ASSESSMENT PROCEDURE: CP-4(3).1		

Assessment Objective

Determine if:

(i) the organization employs automated mechanisms for contingency plan testing/exercises; and

(ii) the automated mechanisms improve the effectiveness of the contingency plan testing/exercises.

Assessment Methods And Objects		
	ncy plan; procedures addressing contingency plan testing and exercises; automated mechanisms suppo entation; other relevant documents or records.(Optional)	rting contingency plan testing/exercises;
CP-5 – Contingency Plan Update (High)		
Control		
	nd, if necessary, revised to address system / organizational changes and/or any problems encountered o	luring plan implementation, execution, or
Guidance		
	ion, functions, or business processes supported by the information system. The organization communica iness Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, I	
Applicability: All	References: ARS: CP-5; FISCAM: TSC-1.1, TSC-3.1.5; HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	Related Controls:
ASSESSMENT PROCEDURE: CP-5.1		
Assessment Objective		
Determine if:		
(i) the organization defines the frequency of cont	ingency plan reviews and updates;	
(ii) the organization updates the contingency pla	n in accordance with organization-defined frequency, at least annually; and	
	izational changes identified by the organization or any problems encountered by the organization during	plan implementation, execution, and testing.
Assessment Methods And Objects		
	ncy plan; procedures addressing contingency plan reviews and updates; information system security pla	n; other relevant documents or records.
ASSESSMENT PROCEDURE: CP-5.2		
Assessment Objective		
	essary changes to the contingency plan to other organizational elements with related plans.	
Assessment Methods And Objects		
	ncy plan; procedures addressing contingency plan reviews and updates; other relevant documents or re-	
	ency plan update responsibilities; organizational personnel with mission-related and operational respons	sibilities.
CP-5(0) – Enhancement (High)		
Control		
Review the CP at least every 365 days and upda other conditions that may impact the system CP.	tte, as necessary, to address: system, organizational, or facility changes; problems encountered during p	lan implementation, execution, or testing; or
Applicability: All	References: ARS: CP-5(0); HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	Related Controls:
ASSESSMENT PROCEDURE: CP-5(0).1		
Assessment Objective		
Determine if the organization meets the requiren	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ing enhancement to the baseline control.
Assessment Methods And Objects		
contingency plan reviews and updates); other re		
	ncy plan; procedures addressing contingency plan reviews and updates; other relevant documents or re-	
	pency plan review and update responsibilities; organizational personnel with mission-related and operation	nal responsibilities.
CP-6 – Alternate Storage Site (High)		
Control		
stored in a secure location at an alternate site ac	be established and implemented effectively to permit the storage of CMS information system backup infor ecessible by management and other key personnel. Procedures shall be developed, documented, and in information system operations and the alternate storage site.	
Guidance		
The frequency of information system backups ar	d the transfer rate of backup information to the alternate storage site (if so designated) are consistent with	th the organization's recovery time objectives

and recovery point objectives.		
Applicability: All	References: ARS: CP-6; IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6; PISP: 4.6.6	Related Controls:
ASSESSMENT PROCEDURE: CP-6.1		
Assessment Objective		
Determine if:		
(i) the organization identifies an alternate storage	•	
	tly in place (if needed) to permit storage of information system backup information.	
Assessment Methods And Objects		
	ency plan; procedures addressing alternate storage sites; alternate storage site agreements; other re	levant documents of records.
ASSESSMENT PROCEDURE: CP-6.2		
Assessment Objective		and the second for the second section of the second
	le, accessible, and meets the requirements (including necessary equipment and supplies) to permit the covery time objectives and recovery point objectives.	ne storage of information system backup
Assessment Methods And Objects	covery lime objectives and recovery point objectives.	
	ency plan; procedures addressing alternate storage sites; alternate storage site; other relevant docun	pents or records
Interview: Organizational personnel with alterna		
CP-6(1) – Enhancement (High)		
Control		
	hically separated from the primary processing site, to prevent susceptibility to the same hazards.	
Applicability: All	References: ARS: CP-6(1); FISCAM: TSC-2.1.3; IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(1) Related Controls:
ASSESSMENT PROCEDURE: CP-6(1).1		
Assessment Objective		
Determine if:		
(i) the contingency plan identifies the primary sto	prage site hazards; and	
(ii) the alternate storage site is sufficiently separate	ated from the primary storage site so as not to be susceptible to the same hazards identified at the pl	rimary site.
Assessment Methods And Objects		
	ency plan; procedures addressing alternate storage sites; alternate storage site; other relevant docun	nents or records.
CP-6(2) – Enhancement (High)		
Control		
Ensure that the alternate storage site is configur	ed to facilitate timely and effective recovery operations.	
Applicability: All	References: ARS: CP-6(2); IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(2)	Related Controls:
ASSESSMENT PROCEDURE: CP-6(2).1		
Assessment Objective		
	red to enable timely and effective recovery of system backup information (i.e., meeting recovery time	and recovery point objectives) in accordance w
the provisions of alternate storage site agreeme	nts.	
Assessment Methods And Objects		
Examine: Contingency planning policy; continge records.	ency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate	e storage site; other relevant documents or
CP-6(3) – Enhancement (High)		
Control		
	ternate storage site in the event of an area-wide disruption or disaster and document explicit mitigation	n actions
Applicability: All	References: ARS: CP-6(3); IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(3)	Related Controls:
ASSESSMENT PROCEDURE: CP-6(3).1		
Assessment Objective Determine if:		
	ssibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and	
Pay 0	\mathbf{D}_{acc} 74 of 207	DDSSM Appendix A Attachmer

(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems. **Assessment Methods And Objects** Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records. CP-7 – Alternate Processing Site (High) Control Agreements with an alternate processing site shall be established and implemented to permit the resumption of CMS information system operations for mission critical business functions when the primary processing capabilities are unavailable, and the CP calls for application recovery in place of other accepted processes. Procedures shall be developed, documented, and implemented effectively to establish contingency activities and responsibilities. Guidance Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives References: ARS: CP-7: FISCAM: TSC-3.2.1; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7; PISP: Applicability: All **Related Controls:** 4.6.7 **ASSESSMENT PROCEDURE: CP-7.1** Assessment Objective Determine if: (i) the organization identifies an alternate processing site: (ii) the organization defines the time period within which processing must be resumed at the alternate processing site; and (iii) alternate processing site agreements are currently in place (if needed) to permit the resumption of information system operations for critical mission/business functions within organization-defined time period. Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan; other relevant documents or records. ASSESSMENT PROCEDURE: CP-7.2 Assessment Objective Determine if the alternate processing site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period. **Assessment Methods And Objects** Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records. Interview: Organizational personnel with alternate processing site responsibilities. CP-7(0) – Enhancement (High) Control Ensure all equipment and supplies required for resuming information system operations for critical functions within twelve (12) hours after COOP activation are available at the alternate processing site, or contracts are in place to support delivery to the site. Applicability: All References: ARS: CP-7(0): IRS-1075: 5.6.2.2#1.5: NIST 800-53/53A: CP-7: PISP: 4.6.7 **Related Controls:** ASSESSMENT PROCEDURE: CP-7(0).1 **Assessment Objective** Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** Examine: Contingency planning policy: contingency plan: procedures addressing alternate processing sites: alternate processing site agreements: information system security plan (for organizationdefined time period within which processing must be resumed at the alternate processing site); other relevant documents or records. Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing site; alternate processing site; other relevant documents or records. Interview: Organizational personnel with alternate processing site responsibilities. CP-7(1) – Enhancement (High) Control Ensure the alternate processing site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards. References: ARS: CP-7(1); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(1) Applicability: All **Related Controls:**

ASSESSMENT PROCEDUR	E: CP-7(1).1	
Assessment Objective		
Determine if:		
	ntifies the primary processing site hazards; and	
	site is sufficiently separated from the primary processing site so as not to be susceptible to the same h	nazards identified at the primary site.
Assessment Methods And		
	nning policy; contingency plan; procedures addressing alternate processing sites; alternate processing	site; other relevant documents or records.
CP-7(2) – Enhancement (Hi	gh)	
Control		
	ty problems to the alternate processing site in the event of an area-wide disruption or disaster and outli	
Applicability: All	References: ARS: CP-7(2); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(2)	Related Controls:
ASSESSMENT PROCEDUR	E: CP-7(2).1	
Assessment Objective		
Determine if:	ntifies potential accessibility problems to the alternate processing site in the event of an area-wide disru	untion or dispotery and
	innes potential accessionity problems to the alternate processing site in the event of an area-wide distr ines explicit mitigation actions for potential accessibility problems.	uption of disaster, and
Assessment Methods And		
	nning policy; contingency plan; procedures addressing alternate processing sites; alternate processing	site: other relevant documents or records.
CP-7(3) – Enhancement (Hi		
Control	5··/	
	g site agreements contain appropriate priority-of-service provisions.	
Applicability: All	References: ARS: CP-7(3); FISCAM: TSC-3.2.1; IRS-1075: 5.6.2.2#1.5; NIST 8	Related Controls:
ASSESSMENT PROCEDUR		
Assessment Objective		
	essing site agreements contain priority-of-service provisions in accordance with the organization's available	ability requirements.
Assessment Methods And		
Examine: Contingency plar	nning policy; contingency plan; procedures addressing alternate processing sites; alternate processing	site agreements; other relevant documents or records.
CP-7(4) – Enhancement (Hi	gh)	
Control		
Ensure the alternate proces	sing site is fully configured to support a minimum required operational capability and ready to use as th	ne operational site.
Applicability: All	References: ARS: CP-7(4); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(4)	Related Controls:
SSESSMENT PROCEDUR	E: CP-7(4).1	
Assessment Objective		
	ssing site agreements specify the requirements needed to support the minimum required operational c	capability of the organization.
Assessment Methods And		
	nning policy; contingency plan; procedures addressing alternate processing sites; alternate processing	site; alternate processing site agreements; other relevant
documents or records.		
SSESSMENT PROCEDUR	E: CP-7(4).2	
Assessment Objective		
	rocessing site is configured to support the minimum required operational capability of the organization a	and is ready to use as the operational site.
Assessment Methods And	•	арананан сана.
Evamine: Contingency plan	nning policy; contingency plan; procedures addressing alternate processing sites; alternate processing	site: alternate processing site agreements: other relevant
documents or records.	······································	ene, anemate proceeding ene agreemente, enter referant

Test: Information system at the alternate processing site.

CP-8 – Telecommunications Services (High)	
Control		
	I implemented for alternate communications services capable of restoring adequate communications to a	ccomplish mission critical functions when the
primary operations and communications capabi		
Guidance		
	ecommunications services are provided by a common carrier, the organization requests Telecommunication	tions Service Priority (TSP) for all
	security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).	
Applicability: All	References: ARS: CP-8; FISCAM: TSC-3.2.2; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8; PISP: 4.6.8	Related Controls:
ASSESSMENT PROCEDURE: CP-8.1	4.0.0	
Assessment Objective		
Determine if:		
	ate telecommunications services to support the information system;	
	in which resumption of information system operations must take place; and	
	ments are in place to permit the resumption of telecommunications services for critical mission/business f	unctions within the organization-defined time
period when the primary telecommunications ca		
Assessment Methods And Objects		
•	ency plan; procedures addressing alternate telecommunications services; information system security pla	an: primary and alternate telecommunications
service agreements; other relevant documents		
ASSESSMENT PROCEDURE: CP-8.2		
Assessment Objective		
Determine if:		
	organization are used for national security emergency preparedness; and	
(ii) a common carrier provides telecommunication		
Assessment Methods And Objects		
	ency plan; procedures addressing alternate telecommunications services; primary and alternate telecomr	nunications service agreements: other
relevant documents or records.		numerations service agreements, other
CP-8(0) – Enhancement (High)		
Control		
	within twelve (12) hours when the primary telecommunications capabilities are unavailable.	
	References: ARS: CP-8(0); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8; PISP: 4.6.8	Related Controls:
ASSESSMENT PROCEDURE: CP-8(0).1		
Assessment Objective		
	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ving enhancement to the baseline control.
Assessment Methods And Objects		
Examine: Contingency planning policy; conting	ency plan; procedures addressing alternate telecommunications services; information system security pla	an (for organization-defined time period withir
	ons must take place); primary and alternate telecommunications service agreements; other relevant docu	
	ency plan; procedures addressing alternate telecommunications services; primary and alternate telecomr	nunications service agreements; other
relevant documents or records.		
CP-8(1) – Enhancement (High)		
Control		
Ensure agreements with primary and alternate t	elecommunication service providers include priority-of-service provisions.	
Applicability: All	References: ARS: CP-8(1); FISCAM: TSC-3.2.2; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(1)	Related Controls:
ASSESSMENT PROCEDURE: CP-8(1).1		
Assessment Objective		
•	cations service agreements contain priority-of-service provisions in accordance with the availability requi	rements defined in the organization's
contingency plan.	outions service agreements contain priority or service provisions in accordance with the availability requil	

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

relevant documents of records.		
CP-8(2) – Enhancement (High)		
Control		
Ensure alternate telecommunication providers d	lo not share a single point of failure with primary telecommunications services.	
Applicability: All	References: ARS: CP-8(2); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(2)	Related Controls:
ASSESSMENT PROCEDURE: CP-8(2).1		
Assessment Objective		
Determine if primary and alternate telecommuni	cations services share a single point of failure.	
Assessment Methods And Objects		
	ency plan; procedures addressing alternate telecommunications services; primary and alternate	telecommunications service agreements; other
relevant documents or records.		
	gency planning and plan implementation responsibilities; telecommunications service providers.	
CP-8(3) – Enhancement (High)		
Control		
	oviders are sufficiently separated from the primary telecommunications services, to prevent susc	
	References: ARS: CP-8(3); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(3)	Related Controls:
ASSESSMENT PROCEDURE: CP-8(3).1		
Assessment Objective	· · · · · · · · · · · · · · · · · · ·	
Determine if the alternate telecommunications s hazards identified at the primary site.	ervice provider's site is sufficiently separated from the primary telecommunications service provider	der's site so as not to be susceptible to the same
Assessment Methods And Objects		
	ency plan; procedures addressing alternate telecommunications services; primary and alternate	telecommunications service agreements: alternate
	ary telecommunications service provider's site; other relevant documents or records.	telecommunications service agreements, alternate
	gency planning and plan implementation responsibilities; telecommunications service providers.	
CP-8(4) – Enhancement (High)		
Control		
Ensure that primary and alternate telecommunic	ation service providers have adequate CPs.	
Applicability: All	References: ARS: CP-8(4); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(4)	Related Controls:
ASSESSMENT PROCEDURE: CP-8(4).1		
Assessment Objective		
Determine if the contingency plans for the prima	ry and alternate telecommunications service providers are sufficient to meet the needs of the org	ganization.
Assessment Methods And Objects		
	ency plan; procedures addressing alternate telecommunications services; primary and alternate	telecommunications service agreements; other
relevant documents or records.		
	gency planning, plan implementation, and testing responsibilities; telecommunications service pr	roviders.
	y-of-service provisions of alternate telecommunications service agreements.	
CP-9 – Information System Backup (Hig	gn)	
Control		
(including system state information) contained ir	orting procedures shall be developed, documented, and implemented effectively to enable the bain the CMS information system. The frequency of information system backups and the transfer radio recovery time objectives and recovery point objectives.	
time. Backup copies of CMS data shall be creat	storage capability. Checkpoint capabilities shall be part of any backup operation that updates file ted on a regular basis, and appropriate safeguards shall be implemented to protect the technical all other forms of data, including paper records, shall be created based upon an assessment of the technical structure of technical structure of the technical structure of the technical structure of technical	I and physical security of backup media at the storage

Guidance Suitance The frequency of information system backups and the transfer rate of backup information, the proteining backup information, proteining backup information, there and information is allow a consideration depending on the type of information reacting rate backup information, proteining backup information, there and information is allow a consideration depending on the type of information reacting rate backup information. Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time. The protection of system backup information, witamatic backup information and restart capabilities and consumes large amounts of computer time. The protection of system backup information witamatics beyond the scope of this control. Applicability: All References: ARS: CP-9; FISCAM: TSG 2: 1:1; FISC 1:1; HIPAA: 164.308(a)(7/6)(A), 164.312(c)(1). Related Controls: MA-CMS-1; MiPAA, MiPA ASSESSMENT PROCEDURE: CP-9.1 Assessment Objective Assessment Objective MiPAA, MiPA Assessment Objective Contingency planning policy: contingency plan; procedures addressing information system backup; information system security plan: backup storage location(s); other relevant or records. Assessment Methods And Objects Examine: Contingency planning policy: contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records. Assessment Mathods And Objects Examine: Contingency planning policy: contingency plan; procedures addressing information system backup; procedures, and the designated forcage locations. </th <th>data loss.</th> <th></th> <th></th>	data loss.		
The frequency of information system backups and the transfer rate of backup information to atternate storage sites (if is designated) are consistent with the organization's recovery time of and recovery time of the organization depending on the type of information residing on the backup information for system backup information, protecting backup information from unauhorized disclosure is also a consisteration depending on the type of information residing on the backup media and the FIPS 199 impact level. A norpatic time. The protection of system backup information or granizational assessment of risk guides the use of encryption for the analysis files and consumes large amounts of compute time. The protection of system backup information system backup information by the organization defines the frequency of information systems backup: (ii) the organization defines the trequency of information systems backup: (ii) the organization defines the user-level and system-level information (including system state information) that is required to be backed up; and (iii) the organization defines the user-level and system-level information (including system state information) that is required to be backed up; and (iii) the organization defines the user-level and system-level information (including system state information) in accordance with the organization defines frequency; (ii) the organization backup information in designated locations in accordance with information system backup procedures; and (iii) the organization backup information in designated locations in accordance with information system backup information (including system state information) in accordance with the organization-defined frequency; (ii) the organization backup information in designated locations in accordance with information system backup procedures; and (iii) the organization backup information in designated locations in accordance with information system backup information system security plan; backup storage location(s); other relevant ore	Guidance		
Applicability: All References: ARS: CP-9; FISCAM: TSC-2.1.1, TSC-2.1.3; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1): Related Controls: MA-CMS-1, MP-4, MP-5 ASSESSMENT PROCEDURE: CP-9.1 Assessment Objective MP-4, MP-5 Assessment Objective IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9 MP-4, MP-5 Assessment Objective IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9 MP-4, MP-5 Assessment Methods And Objects Examine: Contingency planting policy: contingency plant; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records. Assessment Methods And Objects Examine: Contingency planting policy: contingency plant; procedures addressing information system backup; information in accordance with the organization-defined frequency; (i) the organization backup planting policy: contingency planting backup information (including system state information) in accordance with the organization-defined frequency; (ii) the organization protective backup planting policy: contingency planting policy: cont	The frequency of information system backups a and recovery point objectives. While integrity an consideration depending on the type of informat	d availability are the primary concerns for system backup information, protecting backup information fron ion residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk g	n unauthorized disclosure is also an important juides the use of encryption for backup
IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9 MP-4, MP-5 ASSESSMENT PROCEDURE: CP-9.1 Assessment Objective Determine if: (i) the organization defines the frequency of information systems backups: (ii) the organization defines the location(s) for storing backup information. Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records ASSESSMENT PROCEDURE: CP-9.2 Assessment Objective Determine if: (i) the organization stores backup information in designated locations in accordance with information system backup; information jin accordance with the organization-defined frequency: (ii) the organization stores backup information at the designated locations in accordance with information system backup procedures; and (iii) the organization stores backup information at the designated storage locations. Assessment Objective Determine if: (i) the organization stores backup information at the designated storage locations. Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or across. CP-9(0) = Enhancement (High) Control Perform full backups to separate media every other day. Perform incremental or differential backups to separate media every other day. Perform incremental or differential backups to sectored fiste. Off-site. Off-	transit is beyond the scope of this control.		
Assessment Objective Determine II: Determine II: Determine II: Determine II: Determine D	Applicability: All		
Determine if. (i) the organization defines the frequency of information systems backups; (ii) the organization defines the user-level and system-level information (including system state information) that is required to be backed up; and (iii) the organization idefines the location(s) for storing backup information. Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records. Assessment Objective Determine if: (i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency; (ii) the organization stores backup information in designated locations in accordance with information system backup procedures; and (iii) the organization protects backup information at the designated storage locations. Assessment Objective Determine if: (i) the organization protects backup information at the designated storage locations. Assessment (Hethods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records. CP-9(0) = Chhancement (High) Control Perform full backups to sparate media every other day. Perform incremental or differential backups to separate media on the intervening day. Backups to include user-level and system information, including system state information, backup; information system security plan; backup site state and on-site backups multiged with name, date, time and action. Perform full backups to sparate media every other day. Perform incremental or differential backups is esperate media on the intervening day. Backups to include user-level and system information, including system backup; pastient backups multiged exite and on-site backups multing environe backups multing environe backups multi	ASSESSMENT PROCEDURE: CP-9.1		
or records. Assessment Objective Assessment Objective Determine if: (i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency; (ii) the organization backs up information in designated locations in accordance with information system backup procedures; and (iii) the organization backs up information at the designated storage locations. Assessment Methods And Objectis Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records. CP-9(0) – Enhancement (High) Control Perform full backups to separate media every other day. Perform incremental or differential backups to separate media on the intervening day. Backups to include user-level and system information (including system state information). Three generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups mm information (including system state information). Applicability: All References: ARS: CP-9(0); HIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: Related Controls: Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline Assessment Methods And Objects Examinine: Contingency	Determine if: (i) the organization defines the frequency of info (ii) the organization defines the user-level and s (iii) the organization identifies the location(s) for Assessment Methods And Objects	ystem-level information (including system state information) that is required to be backed up; and storing backup information.	storage location(s): other relevant documents
ASSESSMENT PROCEDURE: CP-9.2 Assessment Objective Determine if: (i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency; (ii) the organization protects backup information at the designated locations in accordance with information system backup; procedures; and (iii) the organization protects backup information at the designated storage locations. Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records. CP-9(0) - Enhancement (High) Control Perform full backups to separate media every other day. Perform incremental or differential backups to separate media on the intervening day. Backups to include user-level and system information (including system state information). Three generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups mu logged with name, date, time and action. Applicability: All References: ARS: CP-9(0); HIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: Related Controls: Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline System backup; backup brage location(s), other relevant documents or records. </td <td></td> <td></td> <td></td>			
Assessment Objective Determine if: (i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency; (ii) the organization backs up the required user-level and system-level information (including system backup procedures; and (iii) the organization protects backup information at the designated locations in accordance with information system backup procedures; and (iii) the organization protects backup information at the designated storage locations. Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records. CP-9(0) – Enhancement (High) Control Perform full backups to separate media every other day. Perform incremental or differential backups to separate media on the intervening day. Backups to include user-level and system information (including system state information). Three generations of backups (Iuli plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups mulogged with name, date, time and action. Applicability: All References: ARS: CP-9(0); HIPAA: 164.308(a)(7(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: Related Controls: CP-9; PISP: 4.6.9 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline Examine: Contingency planning policy: contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for info system backup): backup storage location(s): other relevant documents or records. CP-9(1) – Enhancement (High) Control Test backup information to verify media reliability and information integrity, following each backup. Applicability: All References: ARS: CP-9(1			
Determine if: ` (i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency; (ii) the organization backs up the required user-level and system-level information in designated locations in accordance with information in accordance with information) in accordance with the organization protects backup information at the designated storage locations. Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant or records. CP-9(0) = Enhancement (High) Control Perform full backups to separate media every other day. Perform incremental or differential backups to separate media on the intervening day. Backups to include user-level and system longaged with name, date, time and action. Applicability: All References: ARS: CP-9(0); FIIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9 Related Controls: Assessment Methods And Objects References: ARS: CP-9(0); TIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: Related Controls: CP-9; PISP: 4.6.9 Related Controls: Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for info system backup); backup storage location(s); other relevant			
ASSESSMENT PROCEDURE: CP-9(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for info system backup); backup storage location(s); other relevant documents or records. CP-9(1) – Enhancement (High) Control Test backup information to verify media reliability and information integrity, following each backup. Applicability: All ASSESSMENT PROCEDURE: CP-9(1).1 Assessment Objective	 (i) the organization backs up the required user-line (ii) the organization stores backup information in (iii) the organization protects backup information Assessment Methods And Objects Examine: Contingency planning policy; contingency records. CP-9(0) – Enhancement (High) Control Perform full backups to separate media every of information (including system state information). logged with name, date, time and action. 	a designated locations in accordance with information system backup procedures; and at the designated storage locations. ency plan; procedures addressing information system backup; information system security plan; backup ther day. Perform incremental or differential backups to separate media on the intervening day. Backup ther day. Perform incremental or differential backups to separate media on the intervening day. Backup ther day. References: ARS: CP-9(0); HIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A:	storage location(s); other relevant documents s to include user-level and system-level e. Off-site and on-site backups must be
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for info system backup); backup storage location(s); other relevant documents or records. CP-9(1) – Enhancement (High) Control Test backup information to verify media reliability and information integrity, following each backup. Applicability: All References: ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1) Related Controls: ASSESSMENT PROCEDURE: CP-9(1).1 Assessment Objective	+ F		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for info system backup); backup storage location(s); other relevant documents or records. CP-9(1) – Enhancement (High) Control Test backup information to verify media reliability and information integrity, following each backup. Applicability: All References: ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1) Related Controls: ASSESSMENT PROCEDURE: CP-9(1).1 Assessment Objective	ASSESSMENT PROCEDURE: CP-9(0).1		
Control Test backup information to verify media reliability and information integrity, following each backup. Applicability: All References: ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1) Related Controls: ASSESSMENT PROCEDURE: CP-9(1).1 Assessment Objective	Determine if the organization meets the requirer Assessment Methods And Objects Examine: Contingency planning policy; conting system backup); backup storage location(s); oth	ency plan; procedures addressing information system backup; information system security plan (for orga	, ,
Test backup information to verify media reliability and information integrity, following each backup. Applicability: All References: ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1) Related Controls: ASSESSMENT PROCEDURE: CP-9(1).1 Assessment Objective Ferences: ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1) Related Controls:	CP-9(1) – Enhancement (High)		
Applicability: All References: ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1) Related Controls: ASSESSMENT PROCEDURE: CP-9(1).1 Assessment Objective Assessment Objective		y and information integrity, following each backup.	
Assessment Objective	· · · · · · · · · · · · · · · · · · ·		Related Controls:
Assessment Objective	ASSESSMENT PROCEDURE: CP-9(1).1		
	Assessment Objective		
Rev. 9 Page 79 of 207 BPSSM Appendix A, At		Page 79 of 207	BPSSM Appendix A, Attachment

(i) the organization defines the					
	(ii) the organization conducts information system backup testing within the organization-defined frequency; and				
	(iii) testing results verify backup media reliability and information integrity.				
Assessment Methods And C	•				
storage location(s); other rel		 plan; procedures addressing information system 	backup; information system security plan;	information system backup test results; backup	
CP-9(2) – Enhancement (Hig		olds.			
Control	J''/				
	on to restore information	n systems as part of the Contingency Plan testing			
Applicability: All		eferences: ARS: CP-9(2); IRS-1075: 5.6.2.2#1.6;		Related Controls:	
ASSESSMENT PROCEDURI					
Assessment Objective					
	n uses selected backup	information in the restoration of information syste	m functions as part of contingency plan tes	sting.	
Assessment Methods And (-	
Examine: Contingency plan documents or records.	ning policy; contingency	v plan; procedures addressing information system	backup; information system backup test re	esults; contingency plan test results; other relevant	
CP-9(3) – Enhancement (Hig	gh)				
Control					
Ensure that backup copies on software.	of the operating system	and other critical information system software are	stored at a separate facility or in a fire-rate	ed container that is not collocated with operational	
Applicability: All	Re	eferences: ARS: CP-9(3); IRS-1075: 5.6.2.2#1.6;	NIST 800-53/53A: CP-9(3)	Related Controls:	
ASSESSMENT PROCEDURI	E: CP-9(3).1				
Assessment Objective					
	n stores backup copies	of operating system and other critical information	system software in a separate facility or in	a fire-rated container that is not collocated with the	
Assessment Methods And (Objects				
Examine: Contingency plan	ning policy; contingency	v plan; procedures addressing information system	backup; backup storage location(s); other	relevant documents or records.	
CP-9(4) – Enhancement (Hig	gh)				
Control					
Protect backup information f	rom unauthorized modi	fication.			
Guidance					
The organization employs a	opropriate mechanisms	(e.g., digital signatures, cryptographic hashes) to	protect the integrity of information system	backups. Protecting the confidentiality of system	
backup information is beyon					
Applicability: All		eferences: ARS: CP-9(4); IRS-1075: 5.6.2.2#1.6;	NIST 800-53/53A: CP-9(4)	Related Controls: MP-4, MP-5	
ASSESSMENT PROCEDURI	E: CP-9(4).1				
Assessment Objective			en et e se la combre de la combre		
		nechanisms to protect the integrity of information	system backup information.		
Assessment Methods And (•		hookup, information system desires desired	nontation, hookun atarogo la setien (s), information	
		plan; procedures addressing information system nentation; other relevant documents or records.	backup; information system design docum	nentation; backup storage location(s); information	
, , , , , , , , , , , , , , , , , , , ,					
Interview: Organizational pe	ersonnel with informatio	n system backup responsibilities.			
Interview: Organizational pe CP-9(PII-1) – Enhancement	ersonnel with informatio	n system backup responsibilities.			
Interview: Organizational pe CP-9(PII-1) – Enhancement Control	ersonnel with informatio (High)				
Interview: Organizational pe CP-9(PII-1) – Enhancement Control	ersonnel with informatio (High) able, copy of PII is avail	n system backup responsibilities. able before movement of servers. aferences: HIPAA: 164.310(d)(2)(iv)		Related Controls:	

ASSESSMENT PROCEDURE: CP-9(PII-1).1

Assessment Objective

Determine if the organization ensures a current and retrievable copy of PII is available before movement of servers.

Assessment Methods And Objects

Examine: PII Server Movement Plan is addresses in the COOP and backup procedures are available. A current copy of PII is available.

Interview: Organizational personnel with PII backup responsibilities to determine if the PII copy is current and retrievable.

Test: Following the data backup and reconstitution procedures for PII, determine if the current copy is retrievable.

CP-10 – Information System Recovery and Reconstitution (High)

Control

Information system recovery and reconstitution mechanisms with supporting procedures shall be developed, documented, and implemented effectively to allow the CMS information system to be recovered and reconstituted to a known secure state after a disruption or failure. Recovery of CMS information systems after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

Guidance

Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Applicability: All	References: ARS: CP-10; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10; PISP: 4.6.10	Related Controls:
	PISP: 4.6.10	

ASSESSMENT PROCEDURE: CP-10.1

Assessment Objective

Determine if the organization identifies the means for capturing the information system's operational state including appropriate system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-10.2

Assessment Objective

Determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

Test: Automated mechanisms implementing information system recovery and reconstitution operations.

CP-10(0) – Enhancement (High)

Control

Secure information system recovery and reconstitution includes, but not limited to:

(a) Reset all system parameters (either default or organization-established),

(b) Reinstall patches,

(c) Reestablish configuration settings,

(d) Reinstall application and system software, and

(e) Fully test the system.

Applicability: All

References: ARS: CP-10(0); NIST 800-53/53A: CP-10; PISP: 4.6.10

Related Controls:

ASSESSMENT PROCEDURE: CP-10(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

rest. / atomatea meenamon	implementing internation system receivery and reconstitution operations.	
CP-10(1) – Enhancement (Hig	Jh)	
Control		
Perform full recovery and rec	onstitution of the information system as part of CP testing.	
Applicability: All	References: ARS: CP-10(1); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10(1)	Related Controls:
ASSESSMENT PROCEDURE	: CP-10(1).1	
Assessment Objective		
Determine if the organization	includes a full recovery and reconstitution of the information system as part of contingency plan testing.	
Assessment Methods And O	bjects	
Examine: Contingency plann	ing policy; contingency plan; procedures addressing information system recovery and reconstitution; contingen	cy plan test procedures; contingency plan test results;
other relevant documents or r	ecords.	
Interview: Organizational per	sonnel with information system recovery and reconstitution responsibilities; organizational personnel with conti	ingency testing responsibilities.

Rev. 9

I

Ĩ

Identification and Authentication (IA) – Technical

IA-1 – Identification and Authentication Policy and Procedures (High)

Control

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

Guidance

The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and SP 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	References: ARS: IA-1; IRS-1075: 5.6.3.1#1.1; NIST 800-53/53A: IA-1; PISP: 4.7.1	Related Controls:
ASSESSMENT PROCEDURE: IA-1.1		

Assessment Objective

Determine if:

(i) the organization develops and documents identification and authentication policy and procedures;

(ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review identification and authentication policy and procedures; and

(iv) the organization updates identification and authentication policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.

Interview: Organizational personnel with identification and authentication responsibilities.

ASSESSMENT PROCEDURE: IA-1.2

Assessment Objective

Determine if:

(i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.

Interview: Organizational personnel with identification and authentication responsibilities.

IA-2 – User Identification and Authentication (High)

Control

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique IA of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

Guidance

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in SP 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST SP 800-63 level 1 compliant. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST SP 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals.

Applicability: All

References: ARS: IA-2; FISCAM: TAC-3.2.A.4, TAN-2.1.4; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS1075: 5.6.3.1#1.2, 5.6.3.3#2.3; NIST 800-53/53A: IA-2; PISP: 4.7.2

ASSESSMENT PROCEDURE: IA-2.1

Assessment Objective

Determine if:

(i) the information system uniquely identifies and authenticates users (or processes acting on behalf of users); and

(ii) authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63 and e-authentication risk assessment results.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; e-authentication risk assessment results; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-2(1) – Enhancement (High)

Control

Not applicable.

 Applicability: All
 References: ARS: IA-2(1); FISCAM: TAN-2.1.7; HIPAA: 164.312(d); IRS-1075: 5.6.3.1#1.2

Related Controls:

IA-2(2) – Enhancement (High) Control

Employ multifactor authentication for local system access that is at least NIST SP 800-63 level 3 compliant.

Applicability: All; Optional for ABMAC, COB, CWF,	References: ARS: IA-2(2); NIST 800-53/53A: IA-2(2)	Related Controls:
DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC,		
SS, ZPIC		

ASSESSMENT PROCEDURE: IA-2(2).1

Assessment Objective

Determine if:

(i) the organization defines the NIST SP 800-63 authentication levels for the information system; and

(ii) the information system employs multifactor authentication for local system access that is NIST SP 800-63 compliant in accordance with the organizational selection of level 3 or level 4.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-2(3) – Enhancement (High)

Control

Employ multifactor authentication for remote system access that is NIST SP 800-63 level 4 compliant.

Applicability: All	References: ARS: IA-2(3); FISCAM: TAN-2.1.7; NIST 800-53/53A: IA-2(3)	Related Controls:
ASSESSMENT DROCEDURE: 1A 2/2) 4		

ASSESSMENT PROCEDURE: IA-2(3).1

Assessment Objective

Determine if:

(i) the organization defines the NIST SP 800-63 authentication levels for the information system; and

(ii) the information system employs multifactor authentication for remote system access that is NIST SP 800-63 level 4 compliant.

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

	ligh)			
Control				
Require the use of unique user				
Applicability: All		nces: ARS: IA-2(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4, TAN 5.6.3.1#1.2	-2.1.4, TAN-2.1.7; IRS-	Related Controls:
ASSESSMENT PROCEDURE: I	A-2(CMS-1).1			·
Assessment Objective				
Determine if the information sys	tem uniquely identifies ar	nd authenticates users (or processes acting on behalf of users).		
Assessment Methods And Obj				
	iated documentation; info	SP 800-63; procedures addressing user identification and authentica ormation system audit records; other relevant documents or records		
		nd authentication responsibilities to determine the use of unique use		
	nplementing identification	n and authentication capability for the information system to determine	ne the use of unique use	r identifiers and system and/or network
authenticators is required. IA-2(CMS-2) – Enhancement (H	liah)			
Control	ngn)			
All passwords shall be encrypte	d in transit and at rest			
Applicability: All		nces: ARS: IA-2(CMS-2); FISCAM: TAC-3.2.A.1, TAC-3.2.A.7; IRS-	1075: 5.6.3.1#1.2	Related Controls:
ASSESSMENT PROCEDURE: I		······································		
	1			
Assessment upiective				
Assessment Objective Determine if authentication leve	s for users (or processes	acting on behalf of users) are consistent NIST SP 800-63.		
Determine if authentication leve	· ·	s acting on behalf of users) are consistent NIST SP 800-63.		
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assoc	ects nentication policy; NIST S	s acting on behalf of users) are consistent NIST SP 800-63. SP 800-63; procedures addressing user identification and authentica ormation system audit records; other relevant documents or records		
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assoc rest.	ects nentication policy; NIST S ciated documentation; info	SP 800-63; procedures addressing user identification and authentica ormation system audit records; other relevant documents or records	to determine all passwor	ds are required to be encrypted in transit and a
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assoc rest. Interview: Organizational perso	ects nentication policy; NIST S iated documentation; info	SP 800-63; procedures addressing user identification and authentica prmation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passw	to determine all passwor words are required to be e	ds are required to be encrypted in transit and a encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assoc rest. Interview: Organizational perso	ects nentication policy; NIST S iated documentation; info nnel with identification ar nplementing identification	SP 800-63; procedures addressing user identification and authentica ormation system audit records; other relevant documents or records	to determine all passwor words are required to be e	ds are required to be encrypted in transit and a encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assocrest. Interview: Organizational persocrest: Automated mechanisms in IA-2(CMS-3) – Enhancement (H	ects nentication policy; NIST S iated documentation; info nnel with identification ar nplementing identification	SP 800-63; procedures addressing user identification and authentica prmation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passw	to determine all passwor words are required to be e	ds are required to be encrypted in transit and a encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assocration rest. Interview: Organizational persocration Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (Hordischer Control	ects mentication policy; NIST S iated documentation; info nnel with identification ar mplementing identification ligh)	SP 800-63; procedures addressing user identification and authentica prmation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passw	to determine all passwor words are required to be e	ds are required to be encrypted in transit and a encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assocration rest. Interview: Organizational persocration Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires user	ects nentication policy; NIST S stated documentation; info nnel with identification ar nplementing identification ligh)	SP 800-63; procedures addressing user identification and authentication system audit records; other relevant documents or records authentication responsibilities to determine to determine all passwin and authentication capability for the information system to determine	to determine all passwor words are required to be e	ds are required to be encrypted in transit and a encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and associ- rest. Interview: Organizational persoci- Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (Hordischer Control	ects hentication policy; NIST S iated documentation; info nnel with identification ar mplementing identification ligh) identification for any trar Referent	SP 800-63; procedures addressing user identification and authentica ormation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passw in and authentication capability for the information system to determine msaction that has information security implications.	to determine all passwor words are required to be e	rds are required to be encrypted in transit and a encrypted in transit and at rest. uired to be encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assocrest. Interview: Organizational persocrest: Automated mechanisms i IA-2(CMS-3) – Enhancement (H Control Help desk support requires user Applicability: All ASSESSMENT PROCEDURE: I	ects hentication policy; NIST S iated documentation; info nnel with identification ar mplementing identification ligh) identification for any trar Referent	SP 800-63; procedures addressing user identification and authentica ormation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passw in and authentication capability for the information system to determine msaction that has information security implications.	to determine all passwor words are required to be e	rds are required to be encrypted in transit and a encrypted in transit and at rest. uired to be encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assocrest. Interview: Organizational persocrest: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires user Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective	ects hentication policy; NIST S ciated documentation; info nnel with identification ar mplementing identification ligh) identification for any trar Referent A-2(CMS-3).1	SP 800-63; procedures addressing user identification and authentica ormation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passw in and authentication capability for the information system to determine msaction that has information security implications.	to determine all passwor words are required to be e	rds are required to be encrypted in transit and a encrypted in transit and at rest. uired to be encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assocrest. Interview: Organizational persocrest: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires user Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if authentication leve	ects hentication policy; NIST S ciated documentation; info nnel with identification ar mplementing identification ligh) identification for any trar Referent A-2(CMS-3).1 Is for users (or processes	SP 800-63; procedures addressing user identification and authenticat ormation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passw in and authentication capability for the information system to determine insaction that has information security implications. Inces: ARS: IA-2(CMS-3)	to determine all passwor words are required to be e	rds are required to be encrypted in transit and a encrypted in transit and at rest. uired to be encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assocrest. Interview: Organizational persocrest: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires user Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if authentication leve Assessment Methods And Obj	ects hentication policy; NIST S ciated documentation; info nnel with identification ar mplementing identification ligh) identification for any trar Referent A-2(CMS-3).1 Is for users (or processes ects	SP 800-63; procedures addressing user identification and authenticat ormation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passw in and authentication capability for the information system to determine insaction that has information security implications. Inces: ARS: IA-2(CMS-3)	to determine all passwor vords are required to be e ne all passwords are requ	rds are required to be encrypted in transit and a encrypted in transit and at rest. uired to be encrypted in transit and at rest.
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and associ- rest. Interview: Organizational persoci- Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires user Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and associ-	ects hentication policy; NIST S ciated documentation; info nnel with identification ar mplementing identification ligh) identification for any trar Referent A-2(CMS-3).1 Is for users (or processes ects hentication policy; NIST S ciated documentation; info	SP 800-63; procedures addressing user identification and authenticatormation system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passwin and authentication capability for the information system to determine asaction that has information security implications. nces: ARS: IA-2(CMS-3) a acting on behalf of users) are consistent NIST SP 800-63.	to determine all passwor vords are required to be ne all passwords are requ	design documentation; information system
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and associ- rest. Interview: Organizational persoci- Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires used Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and associ- transaction that has information	ects hentication policy; NIST S ciated documentation; info nnel with identification ar mplementing identification ligh) identification for any trar Referent A-2(CMS-3).1 Is for users (or processes ects hentication policy; NIST S ciated documentation; info security implications.	SP 800-63; procedures addressing user identification and authentication system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passwin and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system audit records; other relevant documents or records or records and authentication system audit records; other relevant documents or records and authentication system audit records; other relevant documents or records and authentication system audit records; other relevant documents or records and authentication system audit records; other relevant documents or records and authentication system audit records; other relevant documents or records and authentication and authentication system audit records; other relevant documents or records and authentication and authentication and authentication and authentication and authentication and authentication authentication and authentication and authentication and authentication authentication and authentication and authentication and authentication authentication and authentication and authentication authentication authentication and authentication au	to determine all passwor vords are required to be end all passwords are required to determine help desk s	Add are required to be encrypted in transit and a encrypted in transit and at rest. uired to be encrypted in transit and at rest. Related Controls: design documentation; information system support requires user identification for any
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and associ- rest. Interview: Organizational persoci- Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (Help Control Help desk support requires used Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and associ- transaction that has information Interview: Organizational persoci- information security implications	ects hentication policy; NIST S iated documentation; info nnel with identification ar mplementing identification ligh) identification for any trar Referent A-2(CMS-3).1 Is for users (or processes ects hentication policy; NIST S iated documentation; info security implications. nnel with identification ar	SP 800-63; procedures addressing user identification and authentication system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passwin and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication system and authentication security implications. Appendix ARS: IA-2(CMS-3) Appendix ARS:	to determine all passwor vords are required to be en the all passwords are required to all passwords are required to determine help desk s k support requires user in	Ads are required to be encrypted in transit and a encrypted in transit and at rest. Lired to be encrypted in transit and at rest. Related Controls: design documentation; information system support requires user identification for any dentification for any transaction that has
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assod rest. Interview: Organizational perso Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires used Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assod transaction that has information Interview: Organizational perso information security implications Test: Automated mechanisms i	ects hentication policy; NIST S iated documentation; info nnel with identification ar mplementing identification identification for any trar Referent A-2(CMS-3).1 Is for users (or processes ects hentication policy; NIST S iated documentation; info security implications. nnel with identification ar mplementing identification	SP 800-63; procedures addressing user identification and authentication system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passwin and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system audit records; other relevant documents or records or records and authentication system audit records; other relevant documents or records and authentication system audit records; other relevant documents or records and authentication system audit records; other relevant documents or records and authentication system audit records; other relevant documents or records and authentication system audit records; other relevant documents or records and authentication and authentication system audit records; other relevant documents or records and authentication and authentication and authentication and authentication and authentication and authentication authentication and authentication and authentication and authentication authentication and authentication and authentication and authentication authentication and authentication and authentication authentication authentication and authentication au	to determine all passwor vords are required to be en the all passwords are required to all passwords are required to determine help desk s k support requires user in	Ads are required to be encrypted in transit and a encrypted in transit and at rest. Lired to be encrypted in transit and at rest. Related Controls: design documentation; information system support requires user identification for any dentification for any transaction that has
Determine if authentication lever Assessment Methods And Obj Examine: Identification and aut configuration settings and associ- rest. Interview: Organizational persoci- Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires used Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and associ- transaction that has information Interview: Organizational persoci information security implications Test: Automated mechanisms i has information security implications	ects hentication policy; NIST S iated documentation; info nnel with identification ar mplementing identification identification for any trar Referent A-2(CMS-3).1 Is for users (or processes ects hentication policy; NIST S iated documentation; info security implications. nnel with identification ar mplementing identification ions.	SP 800-63; procedures addressing user identification and authentication system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passwin and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication that has information security implications. Inces: ARS: IA-2(CMS-3) a acting on behalf of users) are consistent NIST SP 800-63. BP 800-63; procedures addressing user identification and authentication must be addressed on the information system and it records; other relevant documents or records and authentication responsibilities to determine to determine help des in and authentication capability for the information system to determine to determine to determine help des in and authentication capability for the information system to determine to determine to determine help des in and authentication capability for the information system to determine to determine to determine help des in and authentication capability for the information system to determine to determine to determine help des in and authentication capability for the information system to determine to determ	to determine all passwor vords are required to be en the all passwords are required to all passwords are required to determine help desk s k support requires user in	Ads are required to be encrypted in transit and a encrypted in transit and at rest. Lired to be encrypted in transit and at rest. Related Controls: design documentation; information system support requires user identification for any dentification for any transaction that has
Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assod rest. Interview: Organizational perso Test: Automated mechanisms in IA-2(CMS-3) – Enhancement (H Control Help desk support requires used Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if authentication leve Assessment Methods And Obj Examine: Identification and aut configuration settings and assod transaction that has information Interview: Organizational perso information security implications Test: Automated mechanisms i	ects hentication policy; NIST S iated documentation; info nnel with identification ar mplementing identification identification for any trar Referent A-2(CMS-3).1 Is for users (or processes ects hentication policy; NIST S iated documentation; info security implications. nnel with identification ar mplementing identification ions.	SP 800-63; procedures addressing user identification and authentication system audit records; other relevant documents or records and authentication responsibilities to determine to determine all passwin and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication capability for the information system to determine and authentication that has information security implications. Inces: ARS: IA-2(CMS-3) a acting on behalf of users) are consistent NIST SP 800-63. BP 800-63; procedures addressing user identification and authentication must be addressed on the information system and it records; other relevant documents or records and authentication responsibilities to determine to determine help des in and authentication capability for the information system to determine to determine to determine help des in and authentication capability for the information system to determine to determine to determine help des in and authentication capability for the information system to determine to determine to determine help des in and authentication capability for the information system to determine to determine to determine help des in and authentication capability for the information system to determine to determ	to determine all passwor vords are required to be en the all passwords are required to all passwords are required to determine help desk s k support requires user in	Ads are required to be encrypted in transit and a encrypted in transit and at rest. Lired to be encrypted in transit and at rest. Related Controls: design documentation; information system support requires user identification for any dentification for any transaction that has

Guidance				
The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an				
organizational authentication solution (e.g., IEEE	802. 1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Sec	curity (TLS) authentication) to identify and		
	etworks. The required strength of the device authentication mechanism is determined by the FIPS 199 s	ecurity categorization of the information		
system with higher impact levels requiring strong Applicability: All	er autnentication. References: ARS: IA-3; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	Related Controls:		
	Reletences. ARS. IA-3, IR3-1075. 5.0.5.1#1.2, NIS1 800-55/55A. IA-3, FISF. 4.7.5	Related Controls.		
ASSESSMENT PROCEDURE: IA-3.1				
Assessment Objective				
Determine if: (i) the organization defines specific devices requi	ring identification and authentication before establishing connections to the information system; and			
	cates specific devices identified by the organization before establishing connections.			
Assessment Methods And Objects				
•	; procedures addressing device identification and authentication; information system design documental	tion: device connection reports: information		
system configuration settings and associated do	cumentation; other relevant documents or records.			
Test: Automated mechanisms implementing dev				
IA-3(0) – Enhancement (High)				
Control				
	r a shared secret or digital certificate to identify and authenticate specific devices before establishing a c	onnection.		
Applicability: All	References: ARS: IA-3(0); IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	Related Controls:		
ASSESSMENT PROCEDURE: IA-3(0).1				
Assessment Objective				
Determine if the organization meets the requirem	ents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ing enhancement to the baseline control.		
Assessment Methods And Objects				
	; information system design documentation; procedures addressing device identification and authenticat	ion; device connection reports; information		
, , , , , , , , , , , , , , , , , , , ,	cumentation; other relevant documents or records.			
Test: Automated mechanisms implementing dev	ice identification and authentication.			
IA-4 – Identifier Management (High)				
Control				
• • •	d implemented effectively to manage user identifiers. The procedures shall address processes and cont	rols for:		
4.7.4.1. Identifying each user uniquely;				
4.7.4.2. Verifying the identity of each user;4.7.4.3. Receiving authorization to issue a user id	lentifier from an appropriate organization official:			
4.7.4.4. Ensuring that the user identifier is issued				
4.7.4.5. Disabling user identifier after a specific p				
4.7.4.6. Archiving user identifiers.				
system accounts (i.e., guest and anonymous).	s shall be conducted to ensure the continued need for access to a system. Identifier management shall	not be applicable to shared information		
Guidance				
	d information system accounts (e.g., guest and anonymous accounts). FIPS 201 and SP 800-73, 800-76	and 800-78 specify a personal identity		
	identification and authentication of federal employees and contractors.	, and boo-ro specify a personal identity		
Applicability: All	References: ARS: IA-4; FISCAM: TAC-3.2.A.4, TAN-2.1.4; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-4; PISP: 4.7.4	Related Controls:		
ASSESSMENT PROCEDURE: IA-4.1		1		
Assessment Objective				
Determine if:				
(i) the organization manages user identifiers by u	niquely identifying each user;			
(ii) the organization manages user identifiers by v				
Rev. 9	Page 86 of 207	BPSSM Appendix A, Attachment 1		

(iii) the experimentian managers upor identifiers by	veneriving outborization to issue a user identifier from an entropyiste organization official	
(iii) the organization manages user identifiers by (iv) the organization manages user identifiers by	receiving authorization to issue a user identifier from an appropriate organization official;	
	activity after which a user identifier is to be disabled;	
	v disabling the identifier after the organization-defined time period of inactivity; and	
(vii) the organization manages user identifiers by		
Assessment Methods And Objects		
-	y; procedures addressing identifier management; information system security plan; information system	design documentation; information system
	ation; list of information system accounts; other relevant documents or records.	
ASSESSMENT PROCEDURE: IA-4.2	, , , , , , , , , , , , , , , , , , , ,	
Assessment Objective		
Determine if the organization uses a Personal lo 800-73, 800-76, and 800-78.	dentity Verification (PIV) card token to uniquely identify and authenticate federal employees and contract	ctors in accordance with FIPS 201 and NIST SP
Assessment Methods And Objects		
Examine: Identification and authentication polic	y; procedures addressing identifier management; information system design documentation; FIPS 201	; NIST SP 800-73, 800-76, 800-78; information
, , ,	ocumentation; list of information system accounts; other relevant documents or records.	
Test: Identity verification capability for the inform	nation system and for organizational facilities.	
IA-4(0) – Enhancement (High)		
Control		
Disable user identifiers after 90 days of inactivity	and delete disabled accounts during annual re-certification process.	
Applicability: All	References: ARS: IA-4(0); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.1#2, 5.6.3.2#2.1; NIST 800- 53/53A: IA-4; PISP: 4.7.4	Related Controls: AC-2(3)
ASSESSMENT PROCEDURE: IA-4(0).1		
Assessment Objective		
-	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amp	lifying enhancement to the baseline control.
Assessment Methods And Objects		
-	y; procedures addressing identifier management; information system security plan (for organization-de	fined time period of inactivity after which user
identifier is to be disabled); information system of documents or records.	sesign documentation; information system configuration settings and associated documentation; list of	information system accounts; other relevant
Test: Identity verification capability for the inforn	nation system and for organizational facilities.	
•	y; procedures addressing identifier management; information system design documentation; FIPS 201	; NIST SP 800-73, 800-76, 800-78; information
	cumentation; list of information system accounts; other relevant documents or records.	
IA-4(CMS-1) – Enhancement (High)		
Control		
	ate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for s	
Applicability: All	References: ARS: IA-4(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4; IRS-1075: 5.6.3.1#2	Related Controls: AC-2(CMS-2)
ASSESSMENT PROCEDURE: IA-4(CMS-1).1		
Assessment Objective		
Determine if the organization manages user ider	ntifiers by uniquely identifying each user.	
Assessment Methods And Objects		
Examine: Identification and authentication polic identifier is to be disabled); information system of	y; procedures addressing identifier management; information system security plan (for organization-de design documentation; information system configuration settings and associated documentation; list of inistrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet,	information system accounts; other relevant
	ication and authentication responsibilities to determine system administrators maintain separate user a r system administration activities.	ccounts; one exclusively for standard user
	nation system and for organizational facilities to determine system administrators maintain separate us	er accounts; one exclusively for standard user
Rev. 9	Page 87 of 207	BPSSM Appendix A, Attachment 1

IA-4(CMS-2) – Enhancement (Hig	ap)	
Control	3''/	
	er identifiers, receive prior written approval from the CIO or his/her designated represer	ntative
Applicability: All	References: ARS: IA-4(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: IA		
Assessment Objective		
	within the organization periodically review identification and authentication policy and pr	rocedures
Assessment Methods And Object		
	entication policy and procedures; other relevant documents or records to determine nor	n-CMS entities receive prior written approval from the CIO or his/her
designated representative before		
Interview: Organizational person	nel with identification and authentication management responsibilities to determine nor	n-CMS entities receive prior written approval from the CIO or his/her
designated representative before		
IA-4(FIS-1) – Enhancement (High	h)	
Control		
	actual system users to remove terminated or transferred employees from the system.	
Applicability: All	References: FISCAM: TAC-3.2.A.6	Related Controls:
ASSESSMENT PROCEDURE: IA	-4(FIS-1).1	
Assessment Objective		
	ersonnel files are automatically [or manually] matched with actual system users to remo	ove terminated or transferred employees from the system.
Assessment Methods And Object	cts	
Examine: Documentation of such		
Examine: Pertinent policies and p	procedures.	
Interview: Security managers.		
IA-5 – Authenticator Manager	ment (High)	
Control		
	documented, and implemented effectively to manage user authenticators. The procedu	
	mised, or damaged authenticators; revocation of authenticators; changing default authe	
Users shall not loan or share auth	henticators with other users. Lost or compromised authenticators shall be reported imm	nediately to appropriate authority.
Selection of passwords or other a	authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS	S System Security Level of the information system Automated mechanisms
shall be in place for password-bas	sed authentication, to ensure that the information system:	
	unauthorized disclosure and modification when stored and transmitted;	
4.7.5.2. Prohibits passwords from		
4.7.5.3. Enforces automatic expira		
4.7.5.4. Prohibits password reuse 4.7.5.5. Enforces periodic passwo	e for a specified number of generations; and	
	ard changes	
-	ord changes.	
Guidance	ž	Isars take reasonable measures to safeguard authenticators including
Guidance Information system authenticators	s include, for example, tokens, PKI certificates, biometrics, passwords, and key cards.	
Guidance Information system authenticators maintaining possession of their ind authentication, the information sys	s include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. I idividual authenticators, not loaning or sharing authenticators with others, and reporting rstem: (i) protects passwords from unauthorized disclosure and modification when store	g lost or compromised authenticators immediately. For password-based ad and transmitted; (ii) prohibits passwords from being displayed when entered;
Guidance Information system authenticators maintaining possession of their ind authentication, the information sys (iii) enforces password minimum a	s include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. I ndividual authenticators, not loaning or sharing authenticators with others, and reporting rstem: (i) protects passwords from unauthorized disclosure and modification when store and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified nur	g lost or compromised authenticators immediately. For password-based ad and transmitted; (ii) prohibits passwords from being displayed when entered; nber of generations. For PKI-based authentication, the information system: (i)
Guidance Information system authenticators maintaining possession of their ind authentication, the information sys (iii) enforces password minimum a validates certificates by constructi	s include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. I ndividual authenticators, not loaning or sharing authenticators with others, and reporting rstem: (i) protects passwords from unauthorized disclosure and modification when store and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified nur ting a certification path to an accepted trust anchor; (ii) establishes user control of the co	g lost or compromised authenticators immediately. For password-based ad and transmitted; (ii) prohibits passwords from being displayed when entered; nber of generations. For PKI-based authentication, the information system: (i) orresponding private key; and (iii) maps the authenticated identity to the user
Guidance Information system authenticators maintaining possession of their ind authentication, the information sys (iii) enforces password minimum a validates certificates by constructi account. In accordance with OMB	s include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. I ndividual authenticators, not loaning or sharing authenticators with others, and reporting rstem: (i) protects passwords from unauthorized disclosure and modification when store and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified nur ting a certification path to an accepted trust anchor; (ii) establishes user control of the co B policy and related E-authentication initiatives, authentication of public users accessing	g lost or compromised authenticators immediately. For password-based ad and transmitted; (ii) prohibits passwords from being displayed when entered; nber of generations. For PKI-based authentication, the information system: (i) orresponding private key; and (iii) maps the authenticated identity to the user g federal information systems (and associated authenticator management) may
Guidance Information system authenticators maintaining possession of their ind authentication, the information sys (iii) enforces password minimum a validates certificates by constructi account. In accordance with OMB also be required to protect nonput	s include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. I ndividual authenticators, not loaning or sharing authenticators with others, and reporting /stem: (i) protects passwords from unauthorized disclosure and modification when store and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified nur ting a certification path to an accepted trust anchor; (ii) establishes user control of the co 3 policy and related E-authentication initiatives, authentication of public users accessing ublic or privacy-related information. FIPS 201 and SP 800-73, 800-76, and 800-78 speci	g lost or compromised authenticators immediately. For password-based and transmitted; (ii) prohibits passwords from being displayed when entered; mber of generations. For PKI-based authentication, the information system: (i) orresponding private key; and (iii) maps the authenticated identity to the user g federal information systems (and associated authenticator management) may ify a personal identity verification (PIV) credential for use in the unique
Guidance Information system authenticators maintaining possession of their ind authentication, the information sys (iii) enforces password minimum a validates certificates by constructi account. In accordance with OMB also be required to protect nonput	s include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. I ndividual authenticators, not loaning or sharing authenticators with others, and reporting rstem: (i) protects passwords from unauthorized disclosure and modification when store and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified nur ting a certification path to an accepted trust anchor; (ii) establishes user control of the co B policy and related E-authentication initiatives, authentication of public users accessing	g lost or compromised authenticators immediately. For password-based and transmitted; (ii) prohibits passwords from being displayed when entered; mber of generations. For PKI-based authentication, the information system: (i) orresponding private key; and (iii) maps the authenticated identity to the user g federal information systems (and associated authenticator management) may ify a personal identity verification (PIV) credential for use in the unique ectronic authentication.

ASSESSMENT PROCEDURE: IA-5.1

Assessment Objective

Determine if:

(i) the organization manages information system authenticators by defining initial authenticator content;

(ii) the organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;

(iii) the organization manages information system authenticators by changing default authenticators upon information system installation; and

(iv) the organization manages information system authenticators by changing/refreshing authenticators periodically.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

Test: Automated mechanisms implementing authenticator management functions.

IA-5(0) – Enhancement (High)

Control

For password-based authentication:

(a) Protect passwords from disclosure or modification when stored or transmitted,

(b) Prevent passwords from being displayed when entered,

(c) When using passwords in connection with e-authentication, refer to ARS Appendix A, e-Authentication Standards for further guidance,

- (d) Force users to select a password comprising a minimum of eight (8) alphanumeric and/or special characters with a number embedded in the password,
- (e) Automatically force users (including administrators) to change account and system account passwords every sixty (60) days,

(f) Automatically force users to select six (6) unique passwords prior to reusing a previous one, and

(g) Enforce password lifetime restrictions within a minimum of one (1) day and maximum of sixty (60) days.

Applicability: All	References: ARS: IA-5(0); HIPAA: 164.308(a)(5)(ii)(D); IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	Related Controls:

ASSESSMENT PROCEDURE: IA-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

Test: Automated mechanisms implementing authenticator management functions.

IA-5(FIS-1) – Enhancement (High)

Control

For devices such as tokens or key cards, users: (1) maintain possession of their individual tokens, cards, etc., and (2) understand that they must not loan or share these with others, and must report lost items immediately.

Applicability: All	References: FISCAM: TAC-3.2.A.8	Related Controls:
ASSESSMENT PROCEDURE: IA-5(FIS-1).1		

Assessment Objective

Determine if:

(i) the organizational users maintain possession of their individual devices such as tokens or key cards, etc.; and

(ii) the organizational users understand they must not loan or share their individual tokens, cards, etc., and report lost items immediately.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Token or key card acknowledgment forms.

Interview: Token and/or key card users.

IA-5(DIR-1) – Enhancement (High)

Control

For password-based authentication, passwords are:

1		1
(a) unique for specific individuals, not groups;		
(b) controlled by the assigned user and not subject to disclosure;		
(c) not displayed when entered; (d) shanned every 60 development an individual shannes positions, showing its intraschedi		
(d) changed every 60 days, when an individual changes positions, or when security is breached;		
(e) at least 8 characters in length; (f) must include at least one number, one upper and lower case character, and one special character;		
(g) prohibited from reuse for at least 6 generation (h) prohibited from being changed more than one		
	est. The use of dictionary names or words as passwords is prohibited.	
Applicability: All	References: FISCAM: TAC-3.2.A.1, TAC-3.2.A.2, TAN-2.1.4	Related Controls:
ASSESSMENT PROCEDURE: IA-5(DIR-1).1	Relefences. FISCAWI. TAC-5.2.A.1, TAC-5.2.A.2, TAN-2.1.4	Related Controls.
Assessment Objective		
	sword and user identification as one tool for security in-depth.	
Assessment Methods And Objects		
	y and acceptable user training policy for completeness in meeting the CMS password controls.	
	ation's policy for password and user system identification.	
Test: Using an appropriate system guide or scrip	t check the system password configuration:	
(a) unique for specific individuals, not groups;		
 (b) controlled by the assigned user and not subject (c) not displayed when entered; 	ct to disclosure;	
(d) changed every 60 days, when an individual of	concerns positions, or when security is breached.	
(e) at least 8 characters in length;	langes positions, or when security is breached,	
	and lower case character, and one special character;	
(g) prohibited from reuse for at least 6 generation		
(h) prohibited from being changed more than on	s, e in a 24-hour period: and	
	est. The use of dictionary names or words as passwords is prohibited.	
IA-6 – Authenticator Feedback (High)		
Control		
	I supporting procedures shall be developed, documented, and implemented effectively to obscure fee	dback to users during the authentication process
to protect the information from possible exploitat		
Guidance		
The feedback from the information system does	not provide information that would allow an unauthorized user to compromise the authentication mech	anism. Displaying asterisks when a user types
in a password is an example of obscuring feedba	ck of authentication information.	
Applicability: All	References: ARS: IA-6; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-6; PISP: 4.7.6	Related Controls:
ASSESSMENT PROCEDURE: IA-6.1		
Assessment Objective		
Determine if the information system obscures fe	back of authentication information during the authentication process to protect the information from	cossible exploitation/use by unauthorized
individuals.		
Assessment Methods And Objects		
	; procedures addressing authenticator feedback; information system design documentation; informati	on system configuration settings and associated
documentation; other relevant documents or rec		, , , , , , , , , , , , , , , , , , , ,
Test: Automated mechanisms implementing aut	nenticator feedback.	
IA-6(0) – Enhancement (High)		
Control		
	swords during the authentication process (e.g., display asterisks).	
Applicability: All	References: ARS: IA-6(0): FISCAM: TAC-3.2.A.1: NIST 800-53/53A: IA-6: PISP: 4.7.6	Related Controls:

ASSESSMENT PROCEDURE: IA-6(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing authenticator feedback.

IA-7 – Cryptographic Module Authentication (High)

Control

Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Guidance

The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	References: ARS: IA-7; NIST 800-53/53A: IA-7; PISP: 4.7.7	Related Controls:
ASSESSMENT PROCEDURE: IA-7.1		

Assessment Objective

Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).

Assessment Methods And Objects

Examine: Identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing cryptographic module authentication.

Incident Response (IR) - Operational

IR-1 – Incident Response Policy and Procedures (High)

Control

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed, documented, and implemented effectively to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-61 and current CMS Procedures.

Guidance

The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

		•
	53/53A: IR-1; PISP: 4.8.1	
Applicability: All	References: ARS: IR-1; FISCAM: TSP-3.4; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1; NIST 800-	Related Controls:

ASSESSMENT PROCEDURE: IR-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents incident response policy and procedures;

(ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review incident response policy and procedures; and

(iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.

Interview: Organizational personnel with incident response planning and plan implementation responsibilities.

ASSESSMENT PROCEDURE: IR-1.2

Assessment Objective

Determine if:

(i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.

Interview: Organizational personnel with incident response planning and plan implementation responsibilities.

IR-2 – Incident Response Training (High)

Control

All personnel shall be trained in their IR roles and responsibilities with respect to a CMS information system. Personnel shall receive periodic refresher training in IR procedures.

Guidance

Procedures and incident response training implementation should:

(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:

(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.

(2) Executives must receive training in information security basics and policy level training in security planning and management.

(3) Program and functional managers must receive training in information security basics; management and implementation level training in system/application security management, and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.

(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.

security management; and management and imp (b) Provide the CMS information systems security the systems. (c) Provide information systems security refreshed	onnel must receive training in information security basics; management and imp elementation level training in system/ application life cycle management, risk ma y awareness material/exposure outlined in NIST guidance on IT security awaren er training for employees as frequently as determined necessary, based on the nt change in the information system environment or procedures or when an emp	anagement, and contingency planning. ness and training to all new employees before allowing them access to sensitivity of the information that the employees use or process.
Applicability: All	References: ARS: IR-2; IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-2; PIS	P: 4.8.2 Related Controls:
ASSESSMENT PROCEDURE: IR-2.1		
Assessment Objective		
 (ii) the organization provides incident response tr (iii) incident response training material addresses (iv) the organization defines the frequency of refr 	sonnel with incident response roles and responsibilities; aining to personnel with incident response roles and responsibilities; the procedures and activities necessary to fulfill identified organizational incide esher incident response training; and sponse training in accordance with organization-defined frequency, at least and	
Examine: Incident response policy; procedures a relevant documents or records.	addressing incident response training; incident response training material; inforr t response training and operational responsibilities.	mation system security plan; incident response training records; other
IR-2(0) – Enhancement (High)		
Control		
Provide training on incident response roles and re	esponsibilities of personnel every 365 days	
	References: ARS: IR-2(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-2; F	PISP: 4.8.2 Related Controls:
ASSESSMENT PROCEDURE: IR-2(0).1		
Assessment Methods And Objects Examine: Incident response policy; procedures a refresher incident response training); incident res	ents as specified in the baseline control and the specific CMS requirements as addressing incident response training; incident response training material; inforr ponse training records; other relevant documents or records. t response training and operational responsibilities.	
IR-2(1) – Enhancement (High)		
Control		
Incorporate simulated events as part of incident r	esponse training.	
Applicability: All	References: ARS: IR-2(1); NIST 800-53/53A: IR-2(1)	Related Controls:
ASSESSMENT PROCEDURE: IR-2(1).1		
Assessment Objective	ted events into incident response training to facilitate effective response by per	sonnel in crisis situations.
Assessment Methods And Objects	3	
Examine: Incident response policy; procedures a	addressing incident response training; incident response training material; other	relevant documents or records.
	t response training and operational responsibilities.	
IR-2(2) – Enhancement (High)		
Control		
Employ automated mechanisms to provide a more	e thorough and realistic incident response training environment.	
Applicability: All	References: ARS: IR-2(2); NIST 800-53/53A: IR-2(2)	Related Controls:

Assessment Objective	
Determine if the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environments of the organization employs automated incident environments of the organization employs automated incident environments of the organization employs automated incident environments of the organization envints of the organization environments of	ment.
Assessment Methods And Objects	
Examine: Incident response policy; procedures addressing incident response training; incident response training material; automated mechanisms	s supporting incident response training; other
relevant documents or records.(Optional)	
Interview: Organizational personnel with incident response training and operational responsibilities.(Optional)	
Test: Simulated incident response training events.(Optional)	
IR-3 – Incident Response Testing and Exercises (High)	
Control	
The IR capability for a CMS information system shall be tested periodically using appropriate tests, procedures, automated mechanisms, and exercise	cises to determine the plan's effectiveness. The test
results, procedures, and exercises employed to conduct the test shall be documented.	
Guidance	
NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.	
Applicability: All References: ARS: IR-3; IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3	Related Controls:
ASSESSMENT PROCEDURE: IR-3.1	
Assessment Objective	
Determine if	
(i) the organization defines incident response tests/exercises;	
(ii) the organization defines the frequency of incident response tests/exercises;	
(iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accord	dance with organization-defined frequency; and
(iv) the organization documents the results of incident response tests/exercises.	
Assessment Methods And Objects	
Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises; information system security plan; incident response testing and exercises	ponse testing material; incident response test
results; other relevant documents or records.	ponse testing material; incident response test
	ponse testing material; incident response test
results; other relevant documents or records.	ponse testing material; incident response test
results; other relevant documents or records. IR-3(0) – Enhancement (High)	ponse testing material; incident response test
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control	ponse testing material; incident response test Related Controls:
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations.	
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1	
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective	Related Controls:
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a	Related Controls:
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects	Related Controls:
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of org	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization-
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of org defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant document	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization-
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of org defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant document IR-3(1) – Enhancement (High)	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization-
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of org defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant document IR-3(1) – Enhancement (High) Control	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization-
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of org defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant document IR-3(1) – Enhancement (High) Control Employ automated mechanisms to test / exercise the incident response plan.	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization-
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of org defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant document IR-3(1) – Enhancement (High) Control Employ automated mechanisms to test / exercise the incident response plan. Guidance	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization- ts or records.
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response tests/exercises); incident response testing and exercises; information system security plan (for list of org defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant document IR-3(1) – Enhancement (High) Control Employ automated mechanisms to test / exercise the incident response plan. Guidance Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete covera	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization- ts or records.
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response tests/exercises); incident response testing and exercises; information system security plan (for list of org defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant document IR-3(1) – Enhancement (High) Control Employ automated mechanisms to test / exercise the incident response plan. Guidance Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete covera realistic test/exercise scenarios and environments, and more effectively stressing the response capability.	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization- ts or records.
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing material; incident response test results; other relevant document IR-3(1) – Enhancement (High) Control Employ automated mechanisms to test / exercise the incident response plan. Guidance Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverarealistic test/exercise scenarios and environments, and more effectively stressing the response capability. Applicability: All References: ARS: IR-3(1); NIST 800-53/53A: IR-3(1)	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization- ts or records.
results; other relevant documents or records. IR-3(0) - Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan (for list of org defined frequency of incident response tests/exercises); incident response testing material; incident response test results; other relevant document (R-3(1) - Enhancement (High) Control Employ automated mechanisms to test / exercise the incident response plan. Guidance Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete covera realistic test/exercise scenarios and environments, and more effectively stressing the response capability. Applicability: All References: ARS: IR-3(1); NIST 800-53/53A: IR-3(1) ASSESSMENT PROCEDURE: IR-3(1).1 References: ARS: IR-3(1); NIST 800-53/53A: IR-3(1)	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization- ts or records.
results; other relevant documents or records. IR-3(0) – Enhancement (High) Control Test and/or exercise and document the incident response capability every 365 days, using reviews, analyses, and simulations. Applicability: All References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3 ASSESSMENT PROCEDURE: IR-3(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a Assessment Methods And Objects Examine: Incident response policy; procedures addressing incident response testing material; incident response test results; other relevant document IR-3(1) – Enhancement (High) Control Employ automated mechanisms to test / exercise the incident response plan. Guidance Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverarealistic test/exercise scenarios and environments, and more effectively stressing the response capability. Applicability: All References: ARS: IR-3(1); NIST 800-53/53A: IR-3(1)	Related Controls: amplifying enhancement to the baseline control. ganization-defined tests/exercises and organization ts or records.

(ii) the automated mechanisms supporting incid	lent response testing provide more complete coverage of incident response issues, more realistic test/e	exercise scenarios, and a greater stress on the
incident response capability.		
Assessment Methods And Objects		
	addressing incident response testing and exercises; information system security plan; incident respon	se testing documentation; automated
	s/exercises; other relevant documents or records.	
Interview: Organizational personnel with incide	ent response testing responsibilities.	
IR-4 – Incident Handling (High)		
Control		
	preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to aputer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learned	
Guidance		
Incident-related information can be obtained fro	m a variety of sources including, but not limited to, audit monitoring, network monitoring, physical acce	ss monitoring, and user/administrator reports.
	ned from ongoing incident handling activities into the incident response procedures and implements the	
Applicability: All	References: ARS: IR-4; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4; PISP: 4.8.4	Related Controls: AU-6, PE-6, SI-2
ASSESSMENT PROCEDURE: IR-4.1		
Assessment Objective		
Determine if:	dling capability for security incidents that includes preparation, detection and analysis, containment, era	adication, and recovery: and
(ii) the incident handling capability is consistent		
Assessment Methods And Objects		
•	addressing incident handling; NIST SP 800-61; other relevant documents or records.	
Interview: Organizational personnel with incide		
Test: Incident handling capability for the organi	zation.	
IR-4(1) – Enhancement (High)		
Control		
Employ automated mechanisms to support the	incident handling process.	
Applicability: All	References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1)	Related Controls:
ASSESSMENT PROCEDURE: IR-4(1).1		
Assessment Objective		
	ed mechanisms to support the incident handling process.	
Assessment Methods And Objects	31	
	addressing incident handling; automated mechanisms supporting incident handling; other relevant do	cuments or records.
Interview: Organizational personnel with incide		
IR-4(CMS-1) – Enhancement (High)		
Control		
	urity incident according to CMS Information Security Incident Handling and Breach Notification Procedu	Ires
Applicability: All	References: ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	Related Controls:
ASSESSMENT PROCEDURE: IR-4(CMS-1).1		
Assessment Objective		
Determine if: (i) the organization implements an incident hand (ii) the incident handling capability is consistent	dling capability for security incidents that includes preparation, detection and analysis, containment, era with NIST SP 800-61.	adication, and recovery; and
Assessment Methods And Objects		
Examine: Incident response policy; procedures incident is documented according to the CMS In	addressing incident handling capability; NIST SP 800-61; other relevant documents or records to dete nformation Security Incident Handling and Breach Notification Procedures.	rmine if relevant information related to a security
Rev. 9	Page 95 of 207	BPSSM Appendix A, Attachment 1

	nnel with incident response training and operational responsibilities to determine if re	elevant information related to a secur	rity incident is documented according to the
CMS Information Security Incide IR-4(CMS-2) – Enhancement (H	ent Handling and Breach Notification Procedures.		
Control			
Preserve evidence through tech	nical means, including secured storage of evidence media and "write" protection of e ollow chain of custody for forensic evidence.	evidence media. Use sound forensic	s processes and utilities that support legal
Applicability: All	References: ARS: IR-4(CMS-2); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3		Related Controls:
ASSESSMENT PROCEDURE: II			•
Assessment Objective			
Determine if:			
(i) the organization implements a	an incident handling capability for security incidents that includes preparation, detecti ity is consistent with NIST SP 800-61.	ion and analysis, containment, eradio	cation, and recovery; and
Assessment Methods And Obje	,		
Examine: Incident response pol means, including secured storag for forensic evidence is followed.	licy; procedures addressing incident handling capability; NIST SP 800-61; other relevent of evidence media and "write" protection of evidence media; sound forensics procest.	esses and utilities are used that supp	port legal requirements. A chain of custody
	nnel with incident response training and operational responsibilities to determine if e		
	ection of evidence media; sound forensics processes and utilities are used that supp	ort legal requirements. A chain of cu	istody for forensic evidence is followed.
IR-4(CMS-3) – Enhancement (H	ign)		
Control			
	uring a security incident. Implement security safeguards to reduce risk and vulnerabi		
Applicability: All	References: ARS: IR-4(CMS-3); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3		Related Controls:
ASSESSMENT PROCEDURE: II	R-4(CMS-3).1		
Assessment Objective			
Determine if:			
	an incident handling capability for security incidents that includes preparation, detecti ty is consistent with NIST SP 800-61.	ion and analysis, containment, eradio	cation, and recovery; and
Assessment Methods And Obje			
	licy; procedures addressing incident handling capability; NIST SP 800-61; other relev		ine if the identification of vulnerabilities
, ,	ent and security safeguards are implemented to reduce risk and vulnerability exploit	•	
	nnel with incident response training and operational responsibilities to determine if th reduce risk and vulnerability exploit exposure.	ne identification of vulnerabilities expl	loited during a security incident and security
IR-5 – Incident Monitoring (
Control			
	information system for security events shall be conducted. All events and activities	associated with system performance	shall be monitored for the identification of
	Induser activity that may indicate security threats resulting from user, software, or har		
	sis. All user activities shall be subject to monitoring to verify compliance with this poli		
Guidance			
It is good practice to separate sy	stem performance issues from incident tracking. However, unexplained system per	formance changes can be the result	of a security incident occurring or data
	the system. Checksums or cyclic redundancy checks (CRCs) can help during the ir	nvestigation of these problems. Whil	le useful for error detection, CRCs cannot be
	data correctness in the face of deliberate (rather than random) changes.		
) can cause performance/incident issues. Note: If an attacker (internal or external pe		
	This would give the attacker the ability to take any action on the system that they wa	ant. For example, an attacker could c	change web pages, reformat the hard disk,
and / or add new users to the loc	cal administrators group. ng on an on-going basis can denote trends within the system or network architecture		
Applicability: All	References: ARS: IR-5; FISCAM: TAC-4.2; HIPAA: 164.308(a)(6)(800-53/53A: IR-5; PISP: 4.8.5		Related Controls:
			1

ASSESSMENT PROCEDUR	E: IR-5.1	
Assessment Objective		
-	on tracks and documents information system security incidents on an ongoing basis.	
Assessment Methods And	, , , , , , , , , , , , , , , , , , , ,	
	e policy; procedures addressing incident monitoring; incident response records and documentation; o	ther relevant documents or records.
Interview: Organizational p	personnel with incident monitoring responsibilities.	
	apability for the organization.	
R-5(1) – Enhancement (Hig	h)	
Control		
	isms to assist in tracking and analyzing security incidents.	
Applicability: All	References: ARS: IR-5(1); NIST 800-53/53A: IR-5(1)	Related Controls:
ASSESSMENT PROCEDUR	έ: IR-5(1).1	
Assessment Objective		
Determine if the organization	on employs automated mechanisms to assist in the tracking of security incidents and in the collection	and analysis of incident information.
Assessment Methods And	Objects	
	e policy; procedures addressing incident monitoring; information system design documentation; inform	mation system configuration settings and associated documentation
	pporting incident monitoring; other relevant documents or records.	
•	personnel with incident monitoring responsibilities.	
R-6 – Incident Reporting	g (High)	
Control	a disarity of a shall be associated to the OMO IT Operator Deal (conservation) and shall a feature to the share	and the standard
	ed incidents, shall be reported to the CMS IT Service Desk (or equivalent organizational function) as s systems. Events and confirmed security incidents by business partners shall also be reported to the C	
Guidance		
	nation reported, the content and timeliness of the reports, and the list of designated reporting authoritie	es or organizations are consistent with applicable laws. Executive
Orders, directives, policies,	regulations, standards, and guidance. Organizational officials report cyber security incidents to the U	nited States Computer Emergency Readiness Team (US-CERT) at
	in the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Secu	
	ormation system are reported to appropriate organizational officials in a timely manner to prevent sec	curity incidents. NIST SP 800-61 provides guidance on incident
reporting.		
Applicability: All	References: ARS: IR-6; FISCAM: TAC-4.2; NIST 800-53/53A: IR-6; PISP: 4.8.	.6 Related Controls:
ASSESSMENT PROCEDUR	E: IR-6.1	
Assessment Objective		
Determine if:		
() 0 1 1	y reports incident information to appropriate authorities;	
()	sistent with NIST SP 800-61;	
(iii) the types of incident info regulations, standards, and	ormation reported, the content and timeliness of the reports, and the list of designated reporting is con	nsistent with applicable laws, Executive Orders, directives, policies,
	abilities in the information system are reported to appropriate organizational officials in a timely mann	er to prevent security incidents
Assessment Methods And	, , , , , , , , , , , , , , , , , , , ,	
	e policy; procedures addressing incident reporting; NIST SP 800-61; incident reporting records and de	ocumentation: other relevant documents or records.
	personnel with incident reporting responsibilities.	- ,
Test: Incident reporting cap		
R-6(1) – Enhancement (Hig	yh)	
Control		
	isms to assist in the reporting of security incidents.	
Employ automated meenar	ionio to application reporting of bedanty indicents.	

Assessment Objective		
	on employs automated mechanisms to assist in the reporting of security incidents.	
Assessment Methods And		
	se policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting	; other relevant documents or records.
	personnel with incident reporting responsibilities.	
R-7 – Incident Respons	e Assistance (High)	
Control		
	r equivalent organizational function) shall be in place and shall play an appropriate role in the organization a system. Procedures shall be developed, documented, and implemented effectively to facilitate the incid sers.	
Guidance		
Possible implementations	of incident response support resources in an organization include a help desk or an assistance group and	access to forensics services, when required.
Applicability: All	References: ARS: IR-7; NIST 800-53/53A: IR-7; PISP: 4.8.7	Related Controls:
ASSESSMENT PROCEDU	RE: IR-7.1	
Assessment Objective		
Determine if:		
() U	s an incident response support resource that offers advice and assistance to users of the information syst	tem for the handling and reporting of security incidents; and
	upport resource is an integral part of the organization's incident response capability.	
Assessment Methods And	•	
	e policy; procedures addressing incident response assistance; other relevant documents or records.	
	personnel with incident response assistance and support responsibilities.	
R-7(1) – Enhancement (Hi	gn)	
Control		
	hisms to increase the availability of incident response-related information and support.	
Applicability: All	References: ARS: IR-7(1); NIST 800-53/53A: IR-7(1)	Related Controls:
ASSESSMENT PROCEDU	RE: IR-7(1).1	
Assessment Objective		
0	on employs automated mechanisms to increase the availability of incident response-related information a	nd support for incident response support.
Assessment Methods And	Objects	
•	e policy; procedures addressing incident response assistance; automated mechanisms supporting incide	nt response support and assistance; other relevant documen
records.		

Interview: Organizational personnel with incident response support and assistance responsibilities and organizational personnel that require incident response support and assistance.

Maintenance (MA) - Operational

MA-1 – System Maintenance Policy and Procedures (High)

Control

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

Guidance

The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: MA-1; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-1; PISP: 4.9.1	Related Controls:

ASSESSMENT PROCEDURE: MA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents information system maintenance policy and procedures;

(ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review information system maintenance policy and procedures; and

(iv) the organization updates information system maintenance policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

ASSESSMENT PROCEDURE: MA-1.2

Assessment Objective

Determine if:

(i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-1(FIS-1) – Enhancement (High)

Control

All system software is current, has current and complete documentation, and is still supported by the vendor.

Applicability: All	References: FISCAM: TSS-3.2.5, TSS-3.2.6	Related Controls:
ASSESSMENT DROCEDURE, MA 4/EIS 4) 4		

ASSESSMENT PROCEDURE: MA-1(FIS-1).1

Assessment Objective

Determine if the organization uses current system software with complete documentation and is vendor supported.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Interview: Management and systems programmers about the currency of system software, and the currency and completeness of software documentation.

Interview: System software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.

MA-2 – Controlled Maintenance (High)

Control

Comprehensive maintenance procedures shall be developed, documented, and implemented effectively to conduct controlled periodic on-site and off-site maintenance of the CMS information

systems and of the physical plant within which these information systems reside. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS-approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly.

Guidance

All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Applicability: All; Optional for SS	References: ARS: MA-2; FISCAM: TSC-2.4.1, TSC-2.4.2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2,	Related Controls:
	5.6.2.4#1.3; NIST 800-53/53A: MA-2; PISP: 4.9.2	

ASSESSMENT PROCEDURE: MA-2.1

Assessment Objective

Determine if the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

MA-2(1) – Enhancement (High)		
Control		
Maintain maintenance records for each	information system that includes:	
(a) Date and time of maintenance,		
(b) Name of the individual performing th	e maintenance, name of escort, if applicable,	
(c) Description of the maintenance perfe		
	ed (including identification numbers, if applicable).	
Applicability: All; Optional for SS	References: ARS: MA-2(1); FISCAM: TSC-2.4.3; NIST 800-53/53A: MA-2(1)	Related Controls:
ASSESSMENT PROCEDURE: MA-2(1).1	
Assessment Objective		
Determine if the organization maintains	maintenance records for the information system that include: (i) the date and time of maintenance;	(ii) name of the individual performing the maintenance; (iii)
	ription of the maintenance performed; and (v) a list of equipment removed or replaced (including id	
Assessment Methods And Objects		
-	nce policy; procedures addressing controlled maintenance for the information system; maintenance	e records; other relevant documents or records.
MA-2(2) – Enhancement (High)		
Control		
	ure that maintenance is scheduled and conducted as required, and that a record of maintenance act	tions both needed and complete is un-to-date accurate
and readily available.		
Applicability: All	References: ARS: MA-2(2); NIST 800-53/53A: MA-2(2)	Related Controls:
ASSESSMENT PROCEDURE: MA-2(2).1	
Assessment Objective		
-	utomated mechanisms to schedule and conduct maintenance as required, and to create accurate,	complete, and available records of all maintenance action
both needed and completed.		
Assessment Methods And Objects		
-	nce policy; procedures addressing controlled maintenance for the information system; automated r	echanisms supporting information system maintenance
	ion settings and associated documentation; maintenance records; other relevant documents or reco	
activities, included by bloth configurat		

MA-2(FIS-1) – Enhancement (High)	
Control	
Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintena	
Applicability: All; Optional for SS References: FISCAM: TSC-2.4.4	Related Controls:
ASSESSMENT PROCEDURE: MA-2(FIS-1).1	
Assessment Objective	
Determine if the organization accommodates regular and a reasonable amount of unscheduled maintenance in its data process	ing operations.
Assessment Methods And Objects	
Examine: Maintenance documentation.	
Examine: Pertinent policies and procedures.	
Interview: Data processing and user management.	
MA-2(FIS-2) – Enhancement (High)	
Control	
Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users thus allow given to users so that service is not unexpectedly interrupted.	ling for adequate testing. Advance notification on hardware changes is
Applicability: All References: FISCAM: TSC-2.4.10, TSC-2.4.11	Related Controls:
ASSESSMENT PROCEDURE: MA-2(FIS-2).1	
Assessment Objective	
Determine if:	
(i) the organization schedules hardware equipment and related software changes such to minimize user impact and maximize re	esources for adequate testing; and
(ii) the organizational advance notification for hardware equipment changes does not cause unexpected interrupted user service	es.
Assessment Methods And Objects	
Examine: Pertinent policies and procedures.	
Examine: Supporting documentation.	
Interview: Senior management, data processing management, and user management.	
MA-2(PII-1) – Enhancement (High)	
Control	
In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which a	
Applicability: All References: HIPAA: 164.310(a)(2)(iv)	Related Controls:
ASSESSMENT PROCEDURE: MA-2(PII-1).1	
Assessment Objective	
Determine if the organization documents repairs and modifications to the facility containing PII.	
Assessment Methods And Objects	
Examine: Facility documentation (such as floor plan and elevation drawings) are updated when repairs and modifications cause	
Interview: Organizational personnel, with facility management responsibilities, to determine if facility documents reflect security Test: Facility documentation sample to determine if repairs or modifications document physical security implications when the facility document physical security implications when the	
MA-3 – Maintenance Tools (High)	
Control	petrollad and manifored. Approved tools shall be maintained an an
The use of system maintenance tools, including diagnostic and test equipment and administration utilities, shall be approved, co going basis.	nitoneu, and monitoreu. Approveu toois shall be maintained on an on-
Guidance	
The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/reparts of the information speci	air actions (e.g., a hardware or software packet sniffer that is
introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support inform	ation system maintenance, yet are a part of the system (e.g., the
software implementing "ping," "Is," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet swi	
Applicability: All References: ARS: MA-3; IRS-1075: 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53	BA: MA-3; PISP: 4.9.3 Related Controls:

ASSESSMENT PROCEDURE: MA-3.1		
Assessment Objective		
Determine if:		
() S	itors the use of information system maintenance tools; and	
(ii) the organization maintains maintenance tools	s on an ongoing basis.	
Assessment Methods And Objects		
, , ,	cy; information system maintenance tools and associated documentation; procedur	res addressing information system maintenance tools; maintena
records; other relevant documents or records.		
MA-3(1) – Enhancement (High)		
Control		
	nd test equipment) carried into a facility by maintenance personnel for obvious imp	roper modifications.
Guidance		
Maintenance tools include, for example, diagnos	stic and test equipment used to conduct maintenance on the information system.	
Applicability: All	References: ARS: MA-3(1); NIST 800-53/53A: MA-3(1)	Related Controls:
ASSESSMENT PROCEDURE: MA-3(1).1		
Assessment Objective		
•	enance tools (e.g., diagnostic and test equipment) carried into a facility by maintena	nce personnel for obvious improper modifications.
Assessment Methods And Objects		
-	cy; information system maintenance tools and associated documentation; procedur	es addressing information system maintenance tools: maintena
records; other relevant documents or records.		,
Interview: Organizational personnel with inform	ation system maintenance responsibilities.	
MA-3(2) – Enhancement (High)		
Control		
Check all media containing diagnostic and test p	programs for malicious code before the media is used in the system.	
Applicability: All	References: ARS: MA-3(2); NIST 800-53/53A: MA-3(2)	Related Controls:
ASSESSMENT PROCEDURE: MA-3(2).1		
Assessment Objective		
•	containing diagnostic test programs (e.g., software or firmware used for information	system maintenance or diagnostics) for malicious code before t
media are used in the information system.		
Assessment Methods And Objects		
	cy; information system maintenance tools and associated documentation; procedur	res addressing information system maintenance tools; information
system media containing maintenance programs	s (including diagnostic and test programs); maintenance records; other relevant do	cuments or records.
Interview: Organizational personnel with information		
MA-3(3) – Enhancement (High)		
Control		
	bility of retaining information to ensure that no sensitive information is saved on the	equipment and that the equipment is appropriately sanitized pr
	I, the equipment must remain within the facility or be destroyed, unless an exceptio	
Applicability: All	References: ARS: MA-3(3); NIST 800-53/53A: MA-3(3)	Related Controls:
ASSESSMENT PROCEDURE: MA-3(3).1		
Assessment Objective		
Determine if:		
	e equipment with the capability of retaining information so that no organizational in	formation is written on the equipment or the equipment is
appropriately sanitized before release; and		
	upment within the facility or destroys the equipment if the equipment cannot be sar	itized, unless an appropriate organization official explicitly
authorizes an exception.		
i i		

Assessment Methods And Objects

Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities.

MA-3(4) – Enhancement (High)		
Control		
Employ automated mechanisms to restrict the us	e of maintenance tools to authorized personnel only.	
Applicability: All	References: ARS: MA-3(4); NIST 800-53/53A: MA-3(4)	Related Controls:
ASSESSMENT PROCEDURE: MA-3(4).1		
Assessment Objective		
	mechanisms to restrict the use of maintenance tools to authorized personnel only.	
Assessment Methods And Objects		
mechanisms supporting information system mair records; other relevant documents or records.(O		
Test: Automated mechanisms supporting inform	ation system maintenance activities.(Optional)	
MA-4 – Remote Maintenance (High)		
Control		
	em must be approved by the CIO or his/her designated representative. Remote maintenance procedure trols on remotely executed maintenance and diagnostic activities.	s shall be developed, documented, and
and shall be reviewed periodically by appropriate	ribed in the SSP for the information system. Maintenance records for all remote maintenance, diagnosti organization officials. All sessions and remote connections shall be terminated after the remote mainte re, the passwords shall be changed following each remote maintenance service.	
Guidance		
maintenance and diagnostic tools is consistent w maintenance and diagnostic activities. Other tech strong identification and authentication technique organization (or information system in certain cas accomplish remote maintenance, the organizatio	e conducted by individuals communicating through an external, non-organization-controlled network (e.g. in the organizational policy and documented in the security plan for the information system. The organization aniques and/or controls to consider for improving the security of remote maintenance include: (i) encryptites, such as Level 3 or 4 tokens as described in NIST SP 800-63; and (iii) remote disconnect verification. ses) terminates all sessions and remote connections invoked in the performance of that activity. If passwing n changes the passwords following each remote maintenance service. NIST SP 800-88 provides guidant redia sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.	on maintains records for all remote on and decryption of communications; (ii) When remote maintenance is completed, the rord-based authentication is used to
Applicability: All	References: ARS: MA-4; FISCAM: TAC-2.1.3; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST	Related Controls: IA-2, MP-6
ASSESSMENT PROCEDURE: MA-4.1	800-53/53A: MA-4; PISP: 4.9.4	
Assessment Objective	s, and controls remotely executed maintenance and diagnostic activities, if employed.	
Assessment Methods And Objects		
	y; procedures addressing remote maintenance for the information system; information system design do	cumentation: information system
	tion; maintenance records; other relevant documents or records.	
Interview: Organizational personnel with informa		
MA-4(1) – Enhancement (High)		
Control		
Audit all remote maintenance sessions, and ensu	are that appropriate information security personnel review the maintenance records of the remote sessio	ns.
Applicability: All	References: ARS: MA-4(1); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4(1)	Related Controls:

ASSESSMENT PROCEDURE: MA-4(1).1		
Assessment Objective		
Determine if:		
(i) the organization audits all remote maintenance		
(ii) designated organizational personnel review t	he maintenance records of remote sessions.	
Assessment Methods And Objects		
, , , , , , , , , , , , , , , , , , , ,	by; procedures addressing remote maintenance for the information system; maintenance records; audit r	ecords; other relevant documents or records.
Interview: Organizational personnel with inform	ation system maintenance responsibilities.	
MA-4(2) – Enhancement (High)		
Control		
Document the use of remote diagnostic tools in		
Applicability: All	References: ARS: MA-4(2); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4(2)	Related Controls:
ASSESSMENT PROCEDURE: MA-4(2).1		
Assessment Objective		
Determine if the organization addresses the inst	allation and use of remote maintenance and diagnostic links in the security plan for the information syste	m.
Assessment Methods And Objects		
Examine: Information system maintenance police	cy; procedures addressing remote maintenance for the information system; information system security p	blan; maintenance records; audit records;
other relevant documents or records.		
MA-4(3) – Enhancement (High)		
Control		
	service organizations utilize the same level of security as the CMS system being serviced. If the service	
	ss the component being serviced is removed from the information system and sanitized (with regard to C	
begins. The component is also sanitized (with robe sanitized (e.g., due to a system failure), remo	egard to potentially malicious software) after the service is performed and before being reconnected to the	ne information system. If the system cannot
Applicability: All	References: ARS: MA-4(3); NIST 800-53/53A: MA-4(3)	Related Controls:
ASSESSMENT PROCEDURE: MA-4(3).1		
Assessment Objective		
-	note diagnostic or maintenance services to be performed by a provider that does not implement for its ow	in information system a level of security at
	d on the information system being services to be performed by a provider that does not implement of its ow	
	begins and also sanitized (with regard to potentially malicious software) after the service is performed a	
system.		J.
Assessment Methods And Objects		
	cy; procedures addressing remote maintenance for the information system; service provider contracts an	d/or service level agreements; maintenance
records; audit records; other relevant documents		
, , , , , , , , , , , , , , , , , , ,	ation system maintenance responsibilities; information system maintenance provider.	
MA-4(CMS-1) – Enhancement (High)		
Control		
If remote maintenance is authorized in writing by		
	; utilize strong identification and authentication techniques, such as tokens; and when remote maintenan ication is used during remote maintenance, change the passwords following each remote maintenance s	
Applicability: All	References: ARS: MA-4(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: MA-4(CMS-1).		Related Controls.
Assessment Objective		
	rs, and controls remotely executed maintenance and diagnostic activities, if employed.	
Assessment Methods And Objects	is, and controlo formatory executed maintenance and diagnostic detrifices, in employed.	
•	cy and procedures; other relevant documents or records to determine that remote maintenance is author	ized in writing by the CIO or his/her

designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service. Interview: Organizational personnel with information system maintenance responsibilities to determine that remote maintenance is authorized in writing by the CIO or his/her designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service. MA-5 – Maintenance Personnel (High) Control Maintenance personnel procedures shall be developed, documented, and implemented effectively to control maintenance of CMS information systems. A list of individuals authorized to perform maintenance on the information system shall be maintained. Guidance Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system. Applicability: All References: ARS: MA-5: NIST 800-53/53A: MA-5: PISP: 4.9.5 **Related Controls: ASSESSMENT PROCEDURE: MA-5.1** Assessment Objective Determine if the organization allows only authorized personnel to perform maintenance on the information system. **Assessment Methods And Objects** Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records: other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-5(0) – Enhancement (High) Control Only authorized individuals are allowed to perform maintenance. Ensure maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. Supervise maintenance personnel during the performance of maintenance activities when they do not have the needed access authorizations. References: ARS: MA-5(0): HIPAA: 164.308(a)(3)(ii)(A): NIST 800-53/53A: MA-5: PISP: 4.9.5 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: MA-5(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-6 – Timely Maintenance (High) Control Maintenance services and parts shall be available in a timely manner. Guidance It is good practice to determine the priority of each system based on the criticality of the system for continued business operations. Each system should be prioritized and interconnections between each of the enterprise's systems mapped and dataflow diagrams developed. Next maintenance contracts as well as emergency maintenance considerations will determine needed availability and pre-placement of spare parts. Applicability: All References: ARS: MA-6: NIST 800-53/53A: MA-6: PISP: 4.9.6 **Related Controls: ASSESSMENT PROCEDURE: MA-6.1 Assessment Objective** Determine if: (i) the organization defines key information system components; (ii) the organization defines the time period within which support and spare parts must be obtained after a failure; and

	ort and spare parts for the organization-defined list of key information system components within the	organization-defined time period of failure.
Assessment Methods And Objects		
	icy; procedures addressing timely maintenance for the information system; service provider contract ecurity plan; other relevant documents or records.	ts and/or service level agreements; inventory and
Interview: Organizational personnel with inform	nation system maintenance responsibilities.	
MA-6(0) – Enhancement (High)		
Control		
Obtain maintenance support and spare parts fo four (24) hours of failure.	or CMS critical systems and applications (including Major Applications (MA) and General Support Sy	stems (GSS) and their components) within twenty-
Applicability: All	References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6	Related Controls:
ASSESSMENT PROCEDURE: MA-6(0).1		
Assessment Objective		
	ments as specified in the baseline control and the specific CMS requirements as prescribed in this a	amplifying enhancement to the baseline control.
Assessment Methods And Objects		
, , , , , , , , , , , , , , , , , , ,		.
MA-CMS-1 – Off-site Physical Repair of	Systems (High)	
Control		
	implemented effectively to enable off-site physical repair of systems without compromising security	functionality or confidentiality
Guidance		renotionality of confidentiality.
	view of a system before it is put back into operation when the system has returned from off-site repa	ir. The repaired system should match the approved
Applicability: All	References: ARS: MA-CMS-1; PISP: 4.9.7	Related Controls: AC-19(CMS-1), AC-3, CP-9, SC-12(CMS-1)
ASSESSMENT PROCEDURE: MA-CMS-1.1		CF-9, 3C-12(CM3-1)
o , , ,	ps procedures, documents procedures, and implements off-site repair of systems without compromi	sing security functionality or confidentiality.
	icy and procedures; other relevant documents or records to determine that only authorized personne	el are permitted access to the system for off-site
repair.		el encore te existence el miner efficite nome in
	nation system maintenance responsibilities to determine that only authorized personnel are permitte	
MA-CMS-1(CMS-0) – Enhancement (High)		
Control		
	zed personnel only. Storage media must be removed before shipment for repairs. Unusable storag rformed, check security features to verify they are functioning properly.	e media must be degaussed or destroyed by
Applicability: All	References: ARS: MA-CMS-1(CMS-0); HIPAA: 164.310(d)(2)(i)	Related Controls:
ASSESSMENT PROCEDURE: MA-CMS-1(CI	MS-0).1	
Assessment Objective		
Determine if the organization allows only author	rized personnel perform maintenance on the information system.	
Assessment Methods And Objects	·	
Storage media must be removed before shipme are checked to verify they are functioning prope	icy and procedures; other relevant documents or records to determine that only authorized personnent for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. erly. nation system maintenance responsibilities determine that only authorized personnel are permitted a	After maintenance is performed, security features
Rev Q	Page 106 of 207	RPSSM Annendix A Attachment

removed before shipment for repairs. Unusable they are functioning properly.	storage media must be degaussed or destroyed by authorized personn	el. After maintenance is performe	ed, security features are checked to verify
MA-CMS-2 – On-site Physical Repair of	Systems (High)		
Control			
Controls shall be developed, documented, and i	mplemented effectively to enable on-site physical repair of systems with	out compromising security function	onality or confidentiality.
Guidance		· · ·	· · ·
Management baseline.	iew of a system before it is put back into operation when the system has	completed repairs. The repaired	system should match the approved Change
Storage media control when encrypted may take	References: ARS: MA-CMS-2; PISP: 4.9.8		Related Controls: AC-19(CMS-1), AC-3,
Applicability: All	References: ARS. MA-UMS-2, PISP. 4.9.0		CP-9, SC-12(CMS-1)
ASSESSMENT PROCEDURE: MA-CMS-2.1			
Assessment Objective			
Determine if the organization effectively develop	s procedures, documents procedures, and implements on-site repair of	systems without compromising s	ecurity functionality or confidentiality.
Assessment Methods And Objects			
Examine: Information system maintenance policity repair.	cy and procedures; other relevant documents or records to determine th	at only authorized personnel are	permitted access to the system for on-site
•	ation system maintenance responsibilities to determine that only authori	zed personnel are permitted acce	ess to systems during on-site repair.
MA-CMS-2(CMS-1) – Enhancement (High)		····	
Control			
Access to system for repair must be by authoriz	ed personnel only.		
Applicability: All	References: ARS: MA-CMS-2(CMS-1)		Related Controls:
ASSESSMENT PROCEDURE: MA-CMS-2(CM	IS-1).1		
Assessment Objective			
Determine if the organization allows only author	ized personnel perform maintenance on the information system.		
Assessment Methods And Objects			
	cy and procedures; other relevant documents or records to determine th		
	ation system maintenance responsibilities to determine that only authori	zed personnel perform maintena	nce on the information system.
MA-CMS-2(CMS-2) – Enhancement (High)			
Control			
Physical repair of servers must be within protect	ed environments.		
Applicability: All	References: ARS: MA-CMS-2(CMS-2)		Related Controls:
ASSESSMENT PROCEDURE: MA-CMS-2(CM	IS-2).1		
Assessment Objective			
Determine if the organization performs physical	repair of servers within protected environments.		
Assessment Methods And Objects	•		
	cy and procedures; other relevant documents or records to determine ph	nysical repair of servers is perform	ned within protected environments.
Interview: Organizational personnel with inform	ation system maintenance responsibilities to determine physical repair of	of servers is performed within prot	ected environments.

Media Protection (MP) – Operational

we did i tote choi (wit) = Operatio	, indi	
MP-1 – Media Protection Policy and Pro	ocedures (High)	
Control		
MP controls and procedures shall be developed	l, documented, and implemented effectively to address media access; media labeling; media transport; n	nedia destruction; media sanitization and
clearing; media storage; and disposition of med	ia records. The MP procedures shall be consistent with applicable laws, Executive Orders, directives, po	plicies, regulations, standards, and guidance.
Guidance		
The media protection policy and procedures are	e consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guida	ance. The media protection policy can be
	rity policy for the organization. Media protection procedures can be developed for the security program in	
system, when required. NIST SP 800-12 provid	es guidance on security policies and procedures.	
Applicability: All	References: ARS: MP-1; FISCAM: TAC-3.4; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1; NIST 800- 53/53A: MP-1; PISP: 4.10.1	Related Controls:
ASSESSMENT PROCEDURE: MP-1.1	•	
Assessment Objective		
Determine if:		
(i) the organization develops and documents me	edia protection policy and procedures;	
(ii) the organization disseminates media protect	ion policy and procedures to appropriate elements within the organization;	
(iii) responsible parties within the organization p	eriodically review media protection policy and procedures; and	
(iv) the organization updates media protection p	policy and procedures when organizational review indicates updates are required.	
Assessment Methods And Objects		
Examine: Media protection policy and procedur	res; other relevant documents or records.	
Interview: Organizational personnel with inform		
ASSESSMENT PROCEDURE: MP-1.2		
Assessment Objective		
Determine if:		
	se, scope, roles and responsibilities, management commitment, coordination among organizational entiti	es, and compliance;
(ii) the media protection policy is consistent with	the organization's mission and functions and with applicable laws, directives, policies, regulations, stand	dards, and guidance; and
(iii) the media protection procedures address all	I areas identified in the media protection policy and address achieving policy-compliant implementations	of all associated security controls.
Assessment Methods And Objects		
Examine: Media protection policy and procedur	res; other relevant documents or records.	
Interview: Organizational personnel with inform		
MP-1(PII-1) – Enhancement (High)		
Control		
Semiannual inventories of magnetic tapes contr	aining PII are conducted. The organization accounts for any missing tape containing PII by documenting	the search efforts and notifying the tape
initiator of the loss.		
Applicability: All	References: IRS-1075: 3.2#3.2, 3.2#3.3	Related Controls:
		Related Controls.
ASSESSMENT PROCEDURE: MP-1(PII-1).1	1	
ASSESSMENT PROCEDURE: MP-1(PII-1).1 Assessment Objective		Related Controls.
Assessment Objective Determine if: (i) the organization verifies semiannual inventor		
Assessment Objective Determine if: (i) the organization verifies semiannual inventor	ies of magnetic tapes containing PII. containing PII by documenting the search efforts and notifying the tape initiator of the loss.	
Assessment Objective Determine if: (i) the organization verifies semiannual inventor		
Assessment Objective Determine if: (i) the organization verifies semiannual inventor the organization accounts for any missing tape of Assessment Methods And Objects	containing PII by documenting the search efforts and notifying the tape initiator of the loss.	
Assessment Objective Determine if: (i) the organization verifies semiannual inventor the organization accounts for any missing tape Assessment Methods And Objects Examine: Records of semiannual inventories of		
Assessment Objective Determine if: (i) the organization verifies semiannual inventor the organization accounts for any missing tape Assessment Methods And Objects Examine: Records of semiannual inventories of MP-2 – Media Access (High)	containing PII by documenting the search efforts and notifying the tape initiator of the loss.	
Assessment Objective Determine if: (i) the organization verifies semiannual inventor the organization accounts for any missing tape Assessment Methods And Objects Examine: Records of semiannual inventories of MP-2 – Media Access (High) Control	containing PII by documenting the search efforts and notifying the tape initiator of the loss.	ion is documented.

access attempts and access granted.

T

access attempts and access granted.			
Guidance			
		ernal/removable hard drives, flash/thumb drives, compact disks	
(e.g., paper, microfilm). This control also applie assistants, cellular telephones).	to portable and mobile computing and co	mmunications devices with information storage capability (e.g.	, notebook computers, personal digital
	selection of media and associated inform	ation contained on that media requiring restricted access. Orga	anizations document in policy and procedures,
the media requiring restricted access, individua	authorized to access the media, and the	specific measures taken to restrict access. The rigor with which	h this control is applied is commensurate with
the FIPS 199 security categorization of the info	nation contained on the media. For exam	ble, fewer protection measures are needed for media containin	g information determined by the organization
		ct on the organization or individuals if accessed by other than	authorized personnel. In these situations, it is
assumed that the physical access controls whe			Deleted Controle
Applicability: All	164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1	-3.1.A.6, TAY-4.1.1; HIPAA: 164.308(a)(3)(ii)(A), ; NIST 800-53/53A: MP-2; PISP: 4.10.2	Related Controls:
ASSESSMENT PROCEDURE: MP-2.1			
Assessment Objective			
Determine if the organization restricts access to	information system media to authorized u	sers.	
Assessment Methods And Objects			
Examine: Information system media protection media storage facilities; access control records		ss; access control policy and procedures; physical and enviror	nmental protection policy and procedures;
Interview: Organizational personnel with inforr	ation system media protection responsibil	ties.	
MP-2(1) – Enhancement (High)			
Control			
Employ automated mechanisms to restrict acce	s to media storage areas and to audit acc	ess attempts and access granted.	
Guidance			
This control enhancement is primarily applicabl where some media is stored (e.g., in individual		an organization where a significant volume of media is stored	and is not intended to apply to every location
Applicability: All	References: ARS: MP-2(1); FISCAM: T MP-2(1)	AC-3.2.C.1, TAC-3.2.C.5; IRS-1075: 4.6#1; NIST 800-53/53A:	Related Controls:
ASSESSMENT PROCEDURE: MP-2(1).1			
Assessment Objective			
Determine if:			
(i) the organization employs automated mechan			
(ii) the organization employs automated mecha	isms to audit access attempts and access	granted.	
Assessment Methods And Objects			
Examine: Information system media protection	oolicy; procedures addressing media acce	ss; access control policy and procedures; physical and enviror	nmental protection policy and procedures;
media storage facilities; access control devices Test: Automated mechanisms implementing ac		er relevant documents or records.	
MP-3 – Media Labeling (High)			
Control			
	all have external labels affixed to indicate	the distribution limitations, applicable security classification, a	nd handling caveats of the information.
		irement, so long as the exempted items remain within a secure	
designated representative shall have the autho	ty to exempt specific types of media or ha	rdware components from the labeling requirement.	-
Guidance			
	s control is applied is commensurate with	anizations document in policy and procedures, the media requ the FIPS 199 security categorization of the information contain ic domain or to be publicly releasable.	
Applicability: All		#1, 5.1#1.2, 5.3#2.1-2, 5.3#3; NIST 800-53/53A: MP-3; PISP:	Related Controls:

ASSESSMENT PROCEDURE: MP-3.1

Assessment Objective

Determine if:

(i) the organization defines its protected environment for media labeling requirements;

(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;

(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and (iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security

markings (if any) of the information.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; information system security plan; removable storage media and information system output; other relevant documents or records.

MP-3(CMS-1) – Enhancement (High)

Control

Off-line backup storage media must be marked according to backup rotation schedule for ease of retrieval.

References: ARS: MP-3(CMS-1); IRS-1075: 4.6#1

Related Controls:

ASSESSMENT PROCEDURE: MP-3(CMS-1).1

Assessment Objective

Determine if:

Applicability: All

(i) the organization defines its protected environment for media labeling requirements;

(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;

(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and (iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine that off-line backup storage media is marked according to backup rotation schedule for ease of retrieval.

Interview: Organizational personnel with information system media protection responsibilities to determine off-line backup storage media is marked according to backup rotation schedule for ease of retrieval.

MP-4 – Media Storage (High)

Control

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper, within controlled areas. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security level of the information ever recorded on it until destroyed or sanitized using CMS-approved procedures.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information, and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST SP 800-56 and 800-57 provide guidance on cryptographic key

	key management.	Belated Cantrala: AC 10, CB 0, CB 0(4)
Applicability: All	References: ARS: MP-4; FISCAM: TCC-3.2.4, TCC-3.3.1; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1; NIST 800-53/53A: MP-4; PISP: 4.10.4	Related Controls: AC-19, CP-9, CP-9(4), RA-2, SC-7
ASSESSMENT PROCEDURE: M		,
Assessment Objective		
Determine if:		
0	lled areas for information system media;	
., .	ocuments the media and associated information contained on that media requiring physical protection in accordance w	ith an organizational assessment of risk;
() S	pecific measures used to protect the selected media and information contained on that media;	
	ntrols and securely stores information system media within controlled areas; and nation system media commensurate with the FIPS 199 security categorization of the information contained on the mec	lia
Assessment Methods And Obje		
	dia protection policy; procedures addressing media storage; physical and environmental protection policy and procedu	res: access control policy and procedures:
	information system media; other relevant documents or records.	
MP-4(PII-1) – Enhancement (Hig	n)	
Control		
Evaluate employing an approved	method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest, consistent with NIST SI	
Applicability: All	References: HIPAA: 164.312(a)(2)(iv)	Related Controls: SC-13
ASSESSMENT PROCEDURE: M	2-4(PII-1).1	
Assessment Objective		
•	s approved cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest.	
Assessment Methods And Obje		
	e licenses used to protect PII at rest. Cryptography software is consistent with NIST SP 800-66 guidance and FIPS 140) approved.
	determine if FIPS 140 approved cryptographic software/system for PII data at rest protection is being used.	
MP-4(PII-2) – Enhancement (Hig	n)	
Control	die with other date. It also dat he waste stad as if it was entirely a super ally identifiable information.	
Applicability: All	dia with other data, it should be protected as if it were entirely personally identifiable information. References: IRS-1075: 5.3#2.3, 5.3#3	Related Controls:
ASSESSMENT PROCEDURE: M		Related Controls:
	4(FII-2).1	
Assessment Objective	ects, in its entirety, personally identifiable information when on magnetic media with other data.	
Assessment Methods And Obje		
Examine: Magnetic storage of P	is protected to determine in its entirety, it is controlled as Federal tax information	
	l is protected to determine, in its entirety, it is controlled as Federal tax information. determine if PII in its entirety is protected as personally identifiable information.	
Interview: Organizational staff to	determine if PII in its entirety is protected as personally identifiable information.	
	determine if PII in its entirety is protected as personally identifiable information.	
Interview: Organizational staff to MP-5 – Media Transport (Hig Control	determine if PII in its entirety is protected as personally identifiable information. (h) nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic)) to authorized personnel based on the
Interview: Organizational staff to MP-5 – Media Transport (Hig Control Physical, administrative, and tech sensitivity of the CMS information	determine if PII in its entirety is protected as personally identifiable information. (h) nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic)) to authorized personnel based on the
Interview: Organizational staff to MP-5 – Media Transport (Hig Control Physical, administrative, and tech sensitivity of the CMS information Guidance Information system media included	determine if PII in its entirety is protected as personally identifiable information. (h) nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) s both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disk	s) and non-digital media (e.g., paper,
Interview: Organizational staff to MP-5 – Media Transport (Hig Control Physical, administrative, and tech sensitivity of the CMS information Guidance Information system media included microfilm). A controlled area is an	determine if PII in its entirety is protected as personally identifiable information. (h) nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) s both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disk y area or space for which the organization has confidence that the physical and procedural protections provided are su	s) and non-digital media (e.g., paper, ifficient to meet the requirements establishe
Interview: Organizational staff to MP-5 – Media Transport (Hig Control Physical, administrative, and tech sensitivity of the CMS information Guidance Information system media included microfilm). A controlled area is an for protecting the information and	determine if PII in its entirety is protected as personally identifiable information. (h) nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) s both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disk y area or space for which the organization has confidence that the physical and procedural protections provided are su for information system. This control also applies to portable and mobile computing and communications devices with in	s) and non-digital media (e.g., paper, ifficient to meet the requirements establishe formation storage capability (e.g., notebook
Interview: Organizational staff to MP-5 – Media Transport (Hig Control Physical, administrative, and tech sensitivity of the CMS information Guidance Information system media include microfilm). A controlled area is an for protecting the information and computers, personal digital assis	determine if PII in its entirety is protected as personally identifiable information. (h) nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) s both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disk y area or space for which the organization has confidence that the physical and procedural protections provided are su for information system. This control also applies to portable and mobile computing and communications devices with in ants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered info	s) and non-digital media (e.g., paper, ifficient to meet the requirements establisher formation storage capability (e.g., notebook rmation systems and may have the capabilit
Interview: Organizational staff to MP-5 – Media Transport (Hig Control Physical, administrative, and tech sensitivity of the CMS information Guidance Information system media include microfilm). A controlled area is an for protecting the information and computers, personal digital assis to store information on internal m	determine if PII in its entirety is protected as personally identifiable information. h) nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) s both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disk y area or space for which the organization has confidence that the physical and procedural protections provided are su for information system. This control also applies to portable and mobile computing and communications devices with in ants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered info edia (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authenticatio	s) and non-digital media (e.g., paper, ifficient to meet the requirements establishe formation storage capability (e.g., notebook rmation systems and may have the capabilit n, and access control mechanisms typically
Interview: Organizational staff to MP-5 – Media Transport (Hig Control Physical, administrative, and tech sensitivity of the CMS information Guidance Information system media include microfilm). A controlled area is ar for protecting the information and computers, personal digital assis to store information on internal m employed in other information system	determine if PII in its entirety is protected as personally identifiable information. (h) nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electronic) s both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disk y area or space for which the organization has confidence that the physical and procedural protections provided are su for information system. This control also applies to portable and mobile computing and communications devices with in ants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered info	s) and non-digital media (e.g., paper, ifficient to meet the requirements establishe formation storage capability (e.g., notebook rmation systems and may have the capabili n, and access control mechanisms typically tems that are transported outside of control

the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for

Applicability: All	References: ARS: MP-5; FISCAM: TAY-4.1.1, TAY-4.1.4; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.6#2, 4.6#4; NIST 800-53/53A: MP-5; PISP: 4.10.5	Related Controls: AC-19, CP-9, CP-9(4)
ASSESSMENT PROCEDURE: M	NP-5.1	
(ii) the organization controls info	sonnel authorized to transport information system media outside of controlled areas; rmation system media during transport outside of controlled areas; and activities associated with transport of information system media to authorized personnel.	
information system security plan	ects edia protection policy; procedures addressing media transport; physical and environmental protection policy and proce ; list of organization-defined personnel authorized to transport information system media outside of controlled areas; in ation system audit records; other relevant documents or records.	
MP-5(1) – Enhancement (High)		
container (e.g., locked briefcase If the use of cryptography is not transport and the information mu in tamper-proof packaging. Correspondence pertaining to a	on digital media are protected during transport outside of controlled areas by using cryptography and tamper proof pack) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier. technically feasible or the sensitive information is stored on non-digital media, written management approval (one level ust be (a) hand carried using securable container via authorized personnel, or (b) if shipped, by United States Postal Se single individual may be mailed through regular USPS mail, but should contain only the minimal amount of sensitive in	below the CIO) must be obtained prior to ervice (USPS) Certified Mail with return receipt
unautnonzed disclosure (e.g., pa	artially masking social security numbers).	
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pro-	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used.	yptographic mechanisms can provide
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pro-	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr	yptographic mechanisms can provide
Guidance Physical and technical security r information residing on the medi	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#2, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1)	yptographic mechanisms can provide
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pro Applicability: All ASSESSMENT PROCEDURE: N Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects digi Assessment Methods And Objective	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#2, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 rity measures (e.g., locked container, cryptography) for information system media transported outside of controlled are tal and non-digital media during transport outside of controlled areas using the organization-defined security measures ects	yptographic mechanisms can provide
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: N Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects digi Assessment Methods And Obje Examine: Information system m information system security plan Interview: Organizational perso	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#2, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) IP-5(1).1 rity measures (e.g., locked container, cryptography) for information system media transported outside of controlled are tal and non-digital media during transport outside of controlled areas using the organization-defined security measures	yptographic mechanisms can provide
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: N Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects digi Assessment Methods And Obje Examine: Information system m information system security plan Interview: Organizational perso	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#2, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) IP-5(1).1 rity measures (e.g., locked container, cryptography) for information system media transported outside of controlled are tal and non-digital media during transport outside of controlled areas using the organization-defined security measures ects ledia protection policy; procedures addressing media transport; physical and environmental protection policy and proce r; information system media transport records; audit records; other relevant documents or records.	yptographic mechanisms can provide
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pro Applicability: All ASSESSMENT PROCEDURE: N Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects digi Assessment Methods And Obje Examine: Information system m information system security plan Interview: Organizational perso MP-5(2) – Enhancement (High) Control	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#2, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) IP-5(1).1 rity measures (e.g., locked container, cryptography) for information system media transported outside of controlled are tal and non-digital media during transport outside of controlled areas using the organization-defined security measures ects ledia protection policy; procedures addressing media transport; physical and environmental protection policy and proce r; information system media transport records; audit records; other relevant documents or records.	yptographic mechanisms can provide
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: M Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects digi Assessment Methods And Obje Examine: Information system m information system security plan Interview: Organizational perso MP-5(2) – Enhancement (High) Control Activities associated with the tra	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) NP-5(1).1 rity measures (e.g., locked container, cryptography) for information system media transported outside of controlled are tal and non-digital media during transport outside of controlled areas using the organization-defined security measures ects ledia protection policy; procedures addressing media transport; physical and environmental protection policy and proce r, information system media transport records; audit records; other relevant documents or records. nnel with information system media transport responsibilities.	yptographic mechanisms can provide B, Related Controls: as; and
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pro Applicability: All ASSESSMENT PROCEDURE: N Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects digi Assessment Methods And Obje Examine: Information system m information system security plan Interview: Organizational perso MP-5(2) – Enhancement (High) Control Activities associated with the tra Guidance Organizations establish docume	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#2 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 rity measures (e.g., locked container, cryptography) for information system media transported outside of controlled are tal and non-digital media during transport outside of controlled areas using the organization-defined security measures ects ects iedia protection policy; procedures addressing media transport; physical and environmental protection policy and proce ; information system media transport records; audit records; other relevant documents or records. nnel with information system media transport responsibilities. nsport of sensitive information system media are documented. ntation requirements for activities associated with the transport of information system media in accordance with the org	yptographic mechanisms can provide B, Related Controls: as; and dures; access control policy and procedures; anizational assessment of risk.
Guidance Physical and technical security r information residing on the medi confidentiality and/or integrity pre- Applicability: All ASSESSMENT PROCEDURE: M Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects digi Assessment Methods And Obje Examine: Information system m information system security plan Interview: Organizational perso MIP-5(2) – Enhancement (High) Control Activities associated with the tra Guidance	neasures for the protection of digital and non-digital media are approved by the organization, commensurate with the F a, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cr otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#2 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 rity measures (e.g., locked container, cryptography) for information system media transported outside of controlled are tal and non-digital media during transport outside of controlled areas using the organization-defined security measures ects ledia protection policy; procedures addressing media transport; physical and environmental protection policy and proce ; information system media transport records; audit records; other relevant documents or records. nnel with information system media transport responsibilities. nsport of sensitive information system media are documented . ntation requirements for activities associated with the transport of information system media in accordance with the org References: ARS: MP-5(2); IRS-1075: 3.2#3.1, 4.4#2, 4.6#2; NIST 800-53/53A: MP-5(2)	yptographic mechanisms can provide 8, Related Controls: as; and dures; access control policy and procedures;

Rev. 9

		I I		
(i) the organization defines a system of records for documenting activities associated with the transport of information system media; and				
(ii) the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records.				
Assessment Methods And Objects				
Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media transport records; audit records; other relevant documents or records.				
MP-5(3) – Enhancement (High)	an media transport records, addit records, other relevant documents of records.			
Control				
Employ an identified custodian at all times to transp	port information system media.			
Guidance	a second the second			
	hts for activities associated with the transport of information system media in accordance with			
	References: ARS: MP-5(3); IRS-1075: 4.4#2, 4.6#2; NIST 800-53/53A: MP-5(3)	Related Controls:		
ASSESSMENT PROCEDURE: MP-5(3).1				
Assessment Objective				
5	I custodian at all times to transport information system media.			
Assessment Methods And Objects				
	licy; procedures addressing media transport; physical and environmental protection policy and	d procedures; information system media transport		
records; audit records; other relevant documents of				
Interview: Organizational personnel with information	on system media transport responsibilities.			
MP-5(PII-1) – Enhancement (High)				
Control				
sealed packing cartons while in transit.	ide of controlled areas and restricts the activities associated with transport of such media to a	uthorized personnel. PII must be in locked cabinets or		
Applicability: All	References: IRS-1075: 4.4#1	Related Controls:		
ASSESSMENT PROCEDURE: MP-5(PII-1).1				
Assessment Objective				
Determine if:				
(i) the organization protects and controls PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel; and				
(ii) the organization uses locked cabinets or sealed packing cartons while PII data is in transit.				
Assessment Methods And Objects				
Examine: Rosters or list of authorized personnel to protect and control PII media during transit.				
Examine: Cabinets or the containers used for protecting PII during transit to determine if there is sufficient fortification to protect PII.				
MP-6 – Media Sanitization and Disposal (I	High)			
Control				
Formal documented procedures shall be developed	d and implemented effectively to ensure that sanitization and disposal methods are commens	surate with the sensitivity and criticality of data residing		
on storage devices, equipment, and hard copy doc to ensure proper functionality.	uments. Media sanitization actions shall be tracked, documented, and verified. Sanitization e	equipment and procedures shall be tested periodically		
	e developed documented and implemented effectively in an environmentally approved man	ner to facilitate the disposal of media, both obstronic		
Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmentally approved manner, to facilitate the disposal of media, both electronic and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. Approved equipment removal procedures for CMS information systems				
	I CMS information shall be followed. Inventory and disposition records for media, both electro			
and retained.				
Guidance				
Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the				
information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to				
unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the				
public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.				
Applicability: All R	References: ARS: MP-6; FISCAM: TAC-3.4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-10	075: Related Controls: MA-4		

	4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2; NIST 800-53/53A: MP-6; PISP: 4.10.6			
ASSESSMENT PROCEDURE: MP-6.1		-		
Assessment Objective				
Determine if: (i) the organization identifies information system	media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the	ne process:		
	on system media, both paper and digital, prior to disposal or release for reuse; and			
(iii) information system media sanitation is consis				
Assessment Methods And Objects				
Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization records; audit records; other relevant documents or records.				
Interview: Organizational personnel with information	ation system media sanitization responsibilities.			
MP-6(0) – Enhancement (High)				
Control				
The sanitization process includes the removal of all data, labels, marking, and activity records using NSA Guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, Guidelines for Media Sanitization.				
Applicability: All	References: ARS: MP-6(0); FISCAM: TAC-3.4; IRS-1075: 8.4#2, 8.4#3; NIST 800-53/53A: MP-6; PISP: 4.10.6	Related Controls:		
ASSESSMENT PROCEDURE: MP-6(0).1				
Assessment Objective				
Determine if the organization meets the requirem	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ying enhancement to the baseline control.		
Assessment Methods And Objects				
Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization records; audit records; other relevant documents or records.				
Interview: Organizational personnel with information	ation system media sanitization responsibilities.			
MP-6(CMS-1) – Enhancement (High)				
Control				
Finely shred, using a minimum of cross-cut shre	dding, hard-copy documents, using approved equipment, techniques, and procedures.			
Applicability: All	References: ARS: MP-6(CMS-1)	Related Controls:		
ASSESSMENT PROCEDURE: MP-6(CMS-1).1				
Assessment Objective				
Determine if:	n in which the state of the state			
(i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process;				
(ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and				
(iii) information system media sanitation is consistent with NIST SP 800-88. Assessment Methods And Objects				
Examine: Media protection policy and procedures; other relevant documents or records to determine hard copy documents are finely shred, using a minimum of cross-cut shredding, using approved				
equipment, techniques, and procedures.				
Interview: Organizational personnel with information system media protection responsibilities to determine hard copy documents are finely shred, using a minimum of cross-cut shredding, using approved equipment, techniques, and procedures.				
MP-6(IRS-1) – Enhancement (High)				
Control				
FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency				
employee. Applicability: All; Optional for ABMAC, CWF, DC, DMFMAC, EDC, DCC, Darth, Darth, CC	References: IRS-1075: 8.4#1	Related Controls:		
DMEMAC, EDC, PSC, PartA, PartB, SS	1			

L				
ASSESSMENT PROCEDURE: MP-6(IRS-1).1				
Assessment Objective				
Determine if:				
., .	ency's agents or contractors during disposal unless authorized by the Internal Revenue Code; and			
(ii) the organization, generally, uses an agency e	employee to witness FTI destruction.			
Assessment Methods And Objects				
Examine: FTI disposal records to determine if u	nauthorized disclose has been given to contractors or other agency agents.			
MP-CMS-1 – Media Related Records (H	igh)			
Control				
Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.				
Guidance				
It is good practice for, electronic, inventory records maintenance that a hash function (a reproducible method of turning inventory data into a (relatively) small number that may serve as a digital "fingerprint" of the data) be performed periodically so that the inventory information can be validated as not being tampered with prior to reconstructive events for an investigation of a possible breach.				
Applicability: All	References: ARS: MP-CMS-1; FISCAM: TCC-3.2.4; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4: PISP: MP-CMS-1	Related Controls:		
ASSESSMENT PROCEDURE: MP-CMS-1.1		<u> </u>		
Assessment Objective				
	y and disposition records for information system media to ensure control and accountability of CMS infor	mation.		
Assessment Methods And Objects				
Examine: Media protection policy and procedure	es; other relevant documents or records to determine inventory and disposition records are maintained for	or information system media to ensure control		
and accountability of CMS information.		,		
	ation system media protection responsibilities to determine inventory and disposition records are maintai	ned for information system media to ensure		
control and accountability of CMS information.				
MP-CMS-1(CMS-0) – Enhancement (High)				
Control				
The media records must, at a minimum, contain:				
(a) The name of media recipient;				
(b) Signature of media recipient;				
(c) Date / time media received;				
(d) Media control number and contents;				
(e) Movement or routing information; and				
(f) If disposed of, the date, time, and method of o		Deleted Original		
Applicability: All	References: ARS: MP-CMS-1(CMS-0); FISCAM: TCC-3.2.4; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4	Related Controls:		
ASSESSMENT PROCEDURE: MP-CMS-1(CM		1		
Assessment Objective				
•	and verifies media sanitization and disposal actions.			
Assessment Methods And Objects				
Examine: Media protection policy and procedures; other relevant documents or records to determine inventory and disposition records are maintained for information system media to ensure control				
and accountability of CMS information. The media records shall contain sufficient information to reconstruct the data in the event of a breach, including but not limited to:				
(a) the name of media recipient;				
(b) signature of media recipient;				
(c) date / time media received;				
(d) media control number and contents;				
(e) movement or routing information; and (f) if disposed of, the date, time, and method of o	lestruction			
Interview: Organizational personnel with information system media protection responsibilities to determine inventory and disposition records are maintained for information system media to ensure				

	The media records shall contain sufficient information to reconstruct the data in the event of a breach, inc	cluding but not limited to:
(a) the name of media recipient;		
(b) signature of media recipient;(c) date / time media received;		
(d) media control number and contents:		
(e) movement or routing information; and		
(f) if disposed of, the date, time, and method of c	destruction.	
MP-CMS-1(PII-1) – Enhancement (High)		
Control		
	ust be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they	must ensure that the proper acknowledgment
form is signed and returned. Inventory records m	nust be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printo	but of a tape, or any file resulting from the
processing of such a tape will be recorded in a lo		
date received		
 reel/cartridge control number contents 		
 number of records, if available 		
• movement, and		
if disposed of, the date and method of dispositi		
	References: IRS-1075: 3.2#1	Related Controls:
ASSESSMENT PROCEDURE: MP-CMS-1(PII-	-1).1	
Assessment Objective		
Determine if:		
	II magnetic tapes/cartridges before, during, and after processing, and the proper acknowledgment form i	s signed and returned; and
	PII control and accountability by a log which contains:	
 date received reel/cartridge control number contents 		
number of records, if available		
• movement, and		
 if disposed of, the date and method of dispositi 	on.	
Assessment Methods And Objects		
Examine: The PII inventory tape/cartridge log for	۱۲-	
date received		
 reel/cartridge control number contents 		
 number of records, if available 		
 movement, and 		
if disposed of, the date and method of dispositi	on.	
MP-CMS-1(IRS-1) – Enhancement (High)		
Control		
	urther disclosures of FTI to their agents or to a contractor unless authorized by statute. (See IRS Pub. 10	
Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	References: IRS-1075: 11.1#1	Related Controls:
ASSESSMENT PROCEDURE: MP-CMS-1(IRS	S-1).1	
Assessment Objective		
Determine if the organization allows unauthorize	d disclosure of FTI data to their agents or to an unauthorized contractor.	
Assessment Methods And Objects		
	rmine is authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7)	
Interview: Organizational staff to determine if pe	ersonnel are knowledgeable of IRS Pub. 1075, sect. 11.1 and 11.7 regarding disclosure of FTI data.	

Physical and Environmental Protection (PE) – Operational

PE-1 – Physical and Environmental Protection Policy and Procedures (High)

Control

Physical and environmental protection procedures shall be developed and implemented effectively to protect all CMS IT infrastructure and assets from unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional. These procedures shall meet all federal, state and local building codes and be consistent with General Services Administration policies, directives, regulations, and guidelines.

Guidance

The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: PE-1; FISCAM: TSC-2.2.6, TSC-2.3.4, TSD-2.1; HIPAA: 164.310(a)(1),	Related Controls:
	164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1; NIST 800-53/53A: PE-1; PISP: 4.11.1	

ASSESSMENT PROCEDURE: PE-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents physical and environmental protection policy and procedures;

(ii) the organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review physical and environmental protection policy and procedures; and

References: FISCAM: TSC-2.2.7

(iv) the organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Physical and environmental protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with physical and environmental protection responsibilities.

ASSESSMENT PROCEDURE: PE-1.2

Assessment Objective

Determine if:

(i) the physical and environmental protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Physical and environmental protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with physical and environmental protection responsibilities.

PE-1(FIS-1) – Enhancement (High)

Control

Eating, drinking, and other behavior that may damage computer equipment is prohibited.

Applicability: All

ASSESSMENT PROCEDURE: PE-1(FIS-1).1

Assessment Objective

Determine if the organization prohibits eating, drinking, and other behavior that may damage computer equipment.

Assessment Methods And Objects

Examine: Employee behavior.

Examine: Employee rules of behavior.

Examine: Pertinent policies and procedures.

Interview: Information system management and users.

Related Controls:

PE-2 – Physical Access Authoriza	ations (High)	
Control		
Access lists of personnel with authorized shall be documented on standard forms	d access to facilities containing CMS information or information systems (except for those areas within the facilities officially des s, maintained on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessary, updated. Ap cards, smart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be removed prompt	propriate authorization
Guidance		<i>,</i>
Appropriate authorization credentials inc to the facility where the information syste	clude, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list perso tem resides.	onnel no longer requiring acces
Applicability: All	References: ARS: PE-2; FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.2, TAC-3.1.A.3, TAC-3.1.A.3,	ntrols:
ASSESSMENT PROCEDURE: PE-2.1		
 (ii) the organization defines the frequence (iii) the organization develops and keeps designated as publicly accessible); (iv) the organization issues appropriate a (v) designated officials within the organization Assessment Methods And Objects Examine: Physical and environmental p or records. PE-2(0) – Enhancement (High) Control 	in the facility that are publicly accessible; cy of review and approval for the physical access list and authorization credentials for the facility; s current lists of personnel with authorized access to the facility where the information system resides (except for those areas w authorization credentials (e.g., badges, identification cards, smart cards); and ization review and approve the access list and authorization credentials at the organization-defined frequency, at least annually. protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credent with authorized access to facilities containing information systems at least once every 90 days. References: ARS: PE-2(0); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-3.1.A.4; NIST 800-53/53A: PE-2; Related Cor	ials; other relevant documents
	PISP: 4.11.2	
ASSESSMENT PROCEDURE: PE-2(0)).1	
Assessment Methods And Objects	requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancem protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credent	
Control		
	or locked room to control access to areas containing PII. These areas will be controlled accordingly.	
Applicability: All	References: IRS-1075: 4.3#1 Related Cor	ntrols:
ASSESSMENT PROCEDURE: PE-2(PI		
(ii) the organization controls a restricted Assessment Methods And Objects Examine: Restricted areas, security roo	area, security room, or locked room to control access to areas containing PII; and I area, security room, or locked room in accordance with BPSSM. oms, or locked rooms that control access to areas containing PII to determine if control and fortification functions are in accordar le for controlling restricted areas, security rooms, or locked rooms containing PII to determine compliance with BPSSM.	nce with BPSSM.

PE-3 – Physical Access Control (High)

Control

Physical access control devices (e.g., keys, locks, combinations, card-readers) and/or guards shall be used to control entry to and exit from facilities containing CMS information or information systems, except for areas and/or facilities officially designated as publicly accessible. Individual access authorizations shall be verified before granting access to facilities containing CMS information or information or information systems. Physical access control devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis.

Combinations, access codes, and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry to facilities during emergency-related events shall be restricted to authorized individuals only. Access to workstations and associated peripheral computing devices shall be appropriately controlled when located in areas designated as publicly accessible.

Guidance

The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control system conforms to the requirements of FIPS 201 and NIST SP 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST SP 800-76.

Applicability: All

References: ARS: PE-3; FISCAM: TAC-3.1.A.3, TAC-3.1.A.5, TAC-3.1.A.7, TAC-3.1.A.8, TAC-3.1.B.2, TAN-2.1.1, TAN-2.1.2, TAN-2.2.1, TSD-2.1; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1; NIST 800-53/53A: PE-3; PISP: 4.11.3

Related Controls:

ASSESSMENT PROCEDURE: PE-3.1

Assessment Objective

Determine if:

(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

(ii) the organization verifies individual access authorizations before granting access to the facility; and

(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records. **Interview:** Organizational personnel with physical access control responsibilities.

Test: Physical access control capability.

ASSESSMENT PROCEDURE: PE-3.2

Assessment Objective

Determine if:

(i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis;

(ii) the organization secures keys, combinations and other access devices on a regular basis; and

(iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records.

Test: Physical access control devices.

ASSESSMENT PROCEDURE: PE-3.3

Assessment Objective

Determine if:

(i) the access control system is consistent with FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed);

(ii) the access control system is consistent with NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and

(iii) the access control system is consistent with NIST SP 800-76 (where the token-based access control function employs biometric verification).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST SP 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records. Test: Physical access control devices. PE-3(1) – Enhancement (High) Control Physical access control to the information system is independent of the physical access controls for the facility. Guidance This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel. Applicability: All References: ARS: PE-3(1): IRS-1075; 4.6#1; NIST 800-53/53A; PE-3(1) **Related Controls: ASSESSMENT PROCEDURE: PE-3(1).1 Assessment Objective** Determine if: (i) the organization identifies specific areas within the facility containing large concentrations of information system components or components requiring additional physical protection; and (ii) for an information system identified as requiring additional physical protection or part of a large concentration of information system components, the organization controls physical access to the system independent of the physical access controls for the facility. Assessment Methods And Objects Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; other relevant documents or records. PE-3(CMS-1) – Enhancement (High) Control Control data center / facility access by use of door and window locks, and security staff or physical authentication devices, such as biometrics and/or smart card / PIN combination. References: ARS: PE-3(CMS-1); IRS-1075; 4,6#1 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: PE-3(CMS-1).1 **Assessment Objective** Determine if the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). Assessment Methods And Objects Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine data center / facility access is controlled by use of door and window locks. Interview: Organizational personnel with physical access control responsibilities to confirm data center / facility access is controlled by use of door and window locks. Test: Physical access control capability to determine data center / facility access is controlled by use of door and window locks. PE-3(CMS-2) – Enhancement (High) Control Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded. References: ARS: PE-3(CMS-2); FISCAM: TAC-3.1.A.5; IRS-1075: 4.6#1 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: PE-3(CMS-2).1 **Assessment Objective** Determine if the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). **Assessment Methods And Objects** Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine servers are stored and operated in physically secure environments protected from unauthorized access.

Interview: Organizational personnel with physical access control responsibilities to determine servers are stored and operated in physically secure environments protected from unauthorized access.

Test: Physical access to Data Center to determin	ne servers are stored and operated in physically secure environments protected from unauthorized acce	ess.
PE-3(CMS-3) – Enhancement (High)		
Control		
Data centers must meet the minimum requirement	nts as established by the Federal Information Systems Control Audit Manual (FISCAM).	
Applicability: All	References: ARS: PE-3(CMS-3); FISCAM: TAC-3.1.A.1, TAN-2.1.1, TAN-2.1.2; IRS-1075: 4.6#1	Related Controls:
ASSESSMENT PROCEDURE: PE-3(CMS-3).1		
Assessment Objective		
Determine if:		
(i) the organization controls all physical access p designated as publicly accessible);	oints (including designated entry/exit points) to the facility where the information system resides (except	for those areas within the facility officially
	horizations before granting access to the facility; and	
	s officially designated as publicly accessible, as appropriate, in accordance with the organization's asses	ssment of risk.
Assessment Methods And Objects		
Examine: Physical and environmental protection	policy; procedures addressing physical access control; physical access control logs or records; other re	elevant documents or records to determine if
	established by the Federal Information Systems Control Audit Manual (FISCAM).	
PE-3(CMS-4) – Enhancement (High)		
Control		
Restrict access to grounds / facilities to authorize	References: ARS: PE-3(CMS-4); IRS-1075: 4.6#1	Related Controls:
Applicability: All ASSESSMENT PROCEDURE: PE-3(CMS-4).1	References: ARS. PE-3(CMS-4), IRS-1075. 4.0#1	Related Controls:
Assessment Objective	a to areas officially designated as publicly accessible, as appropriate in accordance with the arganization	on's apparement of risk
Assessment Methods And Objects	s to areas officially designated as publicly accessible, as appropriate, in accordance with the organization	on's assessment of fisk.
	policy; procedures addressing physical access control; physical access control logs or records; other re	elevant documents or records to determine if
access to grounds / facilities is restricted to autho		
	al access control responsibilities to determine access to grounds / facilities is restricted to authorized per	rsons only.
Test: Physical access controls to determine if ac	cess to grounds / facilities is restricted to authorized persons only.	
PE-3(PII-1) – Enhancement (High)		
Control		
	normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perime	eter/security container. Protected information
	authorized employees may have access after hours.	
	References: IRS-1075: 4.2#2	Related Controls:
ASSESSMENT PROCEDURE: PE-3(PII-1).1		
Assessment Objective		
Determine if:		
	under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked nation in areas where other than authorized employees may have access after hours.	a perimeter/security container; and
Assessment Methods And Objects	nation in areas where other than autionzed employees may have access after hours.	
Examine: Barriers to protect PII to determine two	(2) barriers are present for normal security	
	which protect PII to determine security and fortification during normal hours and after duty hours.	
Interview: Organizational personnel to determine if PII has been disclosed to unauthorized employees.		
	e the effectiveness of protecting PII after hours in secure containers from unauthorized personnel.	
PE-3(DIR-1) – Enhancement (High)		
Control		
Controls are established to protect access autho	rization lists to secure areas such as data centers.	
Applicability: All	References:	Related Controls:

ASSESSMENT PROCEDURE: PE-3(DIR-1).1		
Assessment Objective		
•	d access authorization lists that are for secure areas.	
Assessment Methods And Objects		
	or approved access authorization lists to secure areas.	
PE-4 – Access Control for Transmissio		
Control		
Physical access controls shall be developed, d	ocumented, and implemented effectively to protect against eavesdropping, in-transit modification, disi ganizational facilities that carry unencrypted information.	ruption, and/or physical tampering of CMS
Guidance		
necessary to help prevent eavesdropping or in	tem distribution and transmission lines help prevent accidental damage, disruption, and physical tamp transit modification of unencrypted transmissions. Protective measures to control physical access to i	
	nnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4	Poloted Controlo
Applicability: All ASSESSMENT PROCEDURE: PE-4.1	References: ARS. PE-4, FISUAM. TAU-3.2.E.1, NIST 800-53/53A. PE-4, PISP. 4.11.4	Related Controls:
Assessment Objective		
	access to information system distribution and transmission lines within organizational facilities.	
Assessment Methods And Objects	on policy: procedures addressing access control for transmission medium; information system design	documentation: facility communications and wirin
diagrams; other relevant documents or records	on policy; procedures addressing access control for transmission medium; information system design	documentation, facility communications and with
PE-4(CMS-1) – Enhancement (High)		
Control		
	ation system distribution and transmission lines within organizational facilities only to authorized perso	nnel
Applicability: All	References: ARS: PE-4(CMS-1); FISCAM: TAC-3.2.E.1	Related Controls:
ASSESSMENT PROCEDURE: PE-4(CMS-1).		
Assessment Objective		
•	access to information system distribution and transmission lines within organizational facilities.	
Assessment Methods And Objects		
access to telephone closets and information sy	on policy; procedures addressing physical access control; physical access control logs or records; oth stem distribution and transmission lines within organizational facilities are restricted only to authorized cal access control responsibilities to determine if access to telephone closets and information system thorized personnel.	d personnel.
personnel.	access to telephone closets and information system distribution and transmission lines within organiza	ational facilities are restricted only to authorized
PE-4(CMS-2) – Enhancement (High)		
Control		
Disable any physical ports (e.g., wiring closets,		
Applicability: All	References: ARS: PE-4(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: PE-4(CMS-2).	1	
Assessment Methods And Objects Examine: Physical and environmental protection diagrams; other relevant documents or records Interview: Organizational personnel with physical	access to information system distribution and transmission lines within organizational facilities. on policy; procedures addressing access control for transmission medium; information system design to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. cal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.	
Rev 9	Page 122 of 207	BPSSM Appendix A Attachment

PE-5 – Access Control for Display Med	ium (High)	
Control		
Physical access controls shall be developed, do devices.	ocumented, and implemented effectively to prevent unauthorized individuals from observing CMS sensitiv	e information displayed on information system
Guidance		
It is good practice to position sensitive informat	ion display devices away from windows and areas of ingress and egress.	
Applicability: All	References: ARS: PE-5; FISCAM: TAN-2.1.1; HIPAA: 164.310(b); NIST 800-53/53A: PE-5; PISP: 4.11.5	Related Controls:
ASSESSMENT PROCEDURE: PE-5.1		•
Assessment Objective		
	access to information system devices that display information to prevent unauthorized individuals from ob	serving the display output.
Assessment Methods And Objects		
Examine: Physical and environmental protection records.	on policy; procedures addressing access control for display medium; facility layout of information system of	components; other relevant documents or
PE-6 – Monitoring Physical Access (Hi	igh)	
Control	5 / ·	
Physical access to information systems shall be	e monitored for physical security compliance and to detect and respond to incidents. Appropriate organizations or suspicious physical access activities, and take appropriate remedial action.	ation officials shall periodically review physical
Guidance		
The organization reviews physical access logs part of the organization's incident response cap	periodically and investigates apparent security violations or suspicious physical access activities. Respon ability.	se to detected physical security incidents is
Applicability: All	References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN-2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6	Related Controls: IR-4
ASSESSMENT PROCEDURE: PE-6.1		
Assessment Objective		
Determine if the organization monitors physical	access to the information system to detect and respond to physical security incidents.	
Assessment Methods And Objects		
	on policy; procedures addressing physical access monitoring; physical access logs or records; other relev	ant documents or records.
Interview: Organizational personnel with physi	cal access monitoring responsibilities.	
Test: Physical access monitoring capability.		
PE-6(1) – Enhancement (High)		
Control		
Monitor real-time physical intrusion alarms and		
Applicability: All	References: ARS: PE-6(1); NIST 800-53/53A: PE-6(1)	Related Controls:
ASSESSMENT PROCEDURE: PE-6(1).1		
Assessment Objective		
Determine if the organization monitors real-time	e intrusion alarms and surveillance equipment.	
Assessment Methods And Objects		
Examine: Physical and environmental protection records.	on policy; procedures addressing physical access monitoring; intrusion alarm/surveillance equipment logs	or records; other relevant documents or
Interview: Organizational personnel with physi	cal access monitoring responsibilities.	
PE-6(2) – Enhancement (High)		
Control		
Automated mechanisms are implemented to re	cognize potential intrusions and initiate appropriate response actions.	
Applicability: All	References: ARS: PE-6(2); NIST 800-53/53A: PE-6(2)	Related Controls:

ASSESSMENT PROCEDURE: PE-6(2).1		
Assessment Objective		
	d mechanisms to recognize potential intrusions and initiate appropriate response actions.	
Assessment Methods And Objects		
Examine: Physical and environmental protection	policy; procedures addressing physical access monitoring; information system design documentation; o	ther relevant documents or records.
Test: Automated mechanisms implementing phy	sical access monitoring capability.	
PE-7 – Visitor Control (High)		
Control		
	and implemented effectively to control access to sensitive facilities and restricted / controlled areas control	
	ed prior to being granted access to facilities or areas other than areas designated as publicly accessible.	Government contractors and others with
permanent authorization credentials are not cons	sidered visitors.	
Guidance		
	ent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials frons for the PIV credentials are accredited in accordance with the provisions of NIST SP 800-79.	or federal employees and contractors
Applicability: All	References: ARS: PE-7; FISCAM: TAC-3.1.B.3; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7; PISP: 4.11.7	Related Controls:
ASSESSMENT PROCEDURE: PE-7.1		
Assessment Objective		
	ccess to the information system by authenticating visitors before authorizing access to the facility where	the information system resides other than
areas designated as publicly accessible.		
Assessment Methods And Objects		
Examine: Physical and environmental protection	policy; procedures addressing visitor access control; visitor access control logs or records; other relevant	nt documents or records.
Interview: Organizational personnel with visitor a	access control responsibilities.	
Test: Visitor access control capability.		
PE-7(1) – Enhancement (High)		
Control		
Escort visitors and monitor visitor activity.		
Applicability: All	References: ARS: PE-7(1); FISCAM: TAC-3.1.B.1; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7(1)	Related Controls:
ASSESSMENT PROCEDURE: PE-7(1).1		
Assessment Objective		
Determine if the organization escorts visitors and	I monitors visitor activity, when required.	
Assessment Methods And Objects		
Examine: Physical and environmental protection	policy; procedures addressing visitor access control; visitor access control logs or records; other releval	nt documents or records.
Interview: Organizational personnel with visitor	access control responsibilities.	
PE-7(FIS-1) – Enhancement (High)		
Control		
Visitors, contractors, and maintenance personne	l are authenticated through the use of preplanned appointments and identification checks.	
Applicability: All	References: FISCAM: TAC-3.1.B.3	Related Controls:
ASSESSMENT PROCEDURE: PE-7(FIS-1).1		
Assessment Objective		
•	ors, contractors and maintenance personnel through the use of preplanned appointments and identification	on checks.
Assessment Methods And Objects		
Examine: Appointment and verification procedur	res for visitors.	
Examine: Pertinent policies and procedures.		
Interview: Receptionist or security guard.		
Rev. 9	Page 124 of 207	BPSSM Appendix A. Attachment 1

Control		
Control		
4.11.8.1. Name and organization of t4.11.8.2. Signature of the visitor;4.11.8.3. Form of identification;	nd restricted / controlled areas that contain CMS information or information systems shall be logged. The visito the person visiting;	r access record shall contain:
4.11.8.4. Date of access;		
4.11.8.5. Time of entry and departure	9;	
4.11.8.6. Purpose of visit; and		
4.11.8.7. Name and organization of p	Derson visited.	
Appropriate organization officials sha	all periodically review the access records, including after closeout.	
Guidance		
	d log format for consistency and ease of use during log closeouts and the next months log generation.	
Applicability: All	References: ARS: PE-8; FISCAM: TAC-3.1.B.1, TAC-3.1.B.3; NIST 800-53/53A: PE-8; PISP: 4.1	1.8 Related Controls:
ASSESSMENT PROCEDURE: PE-8	.1	
Assessment Objective		
Determine if:		
(i) the organization defines the frequ	ency of review for visitor access records;	
(ii) the organization maintains visitor includes:	access records to the facility where the information system resides (except for those areas within the facility off	cially designated as publicly accessible) that
- name and organization of the perso	on visiting;	
- signature of the visitor;	-	
 form of identification; 		
 date of access: 		
- time of entry and departure;		
 time of entry and departure; purpose of visit; 	isited and	
 time of entry and departure; purpose of visit; name and organization of person visit; 		
 time of entry and departure; purpose of visit; name and organization of person v (iii) designated officials within the org 	panization review the visitor access logs in accordance with organization-defined frequency.	
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects 	panization review the visitor access logs in accordance with organization-defined frequency.	ess control records: other relevant documents or
 time of entry and departure; purpose of visit; name and organization of person v (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment 	panization review the visitor access logs in accordance with organization-defined frequency.	ess control records; other relevant documents or
 time of entry and departure; purpose of visit; name and organization of person v (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. 	panization review the visitor access logs in accordance with organization-defined frequency.	ess control records; other relevant documents or
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) 	panization review the visitor access logs in accordance with organization-defined frequency.	ess control records; other relevant documents or
time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control	ganization review the visitor access logs in accordance with organization-defined frequency. al protection policy; procedures addressing facility access records; information system security plan; facility acc	ess control records; other relevant documents or
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close 	ganization review the visitor access logs in accordance with organization-defined frequency. al protection policy; procedures addressing facility access records; information system security plan; facility access records; information system security plan; facility access records; and reviewed by management monthly.	
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close Applicability: All 	anization review the visitor access logs in accordance with organization-defined frequency. al protection policy; procedures addressing facility access records; information system security plan; facility access doubted out and reviewed by management monthly. References: ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8	ess control records; other relevant documents or Related Controls:
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close Applicability: All ASSESSMENT PROCEDURE: PE-8 	anization review the visitor access logs in accordance with organization-defined frequency. al protection policy; procedures addressing facility access records; information system security plan; facility access doubted out and reviewed by management monthly. References: ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8	
time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close Applicability: All ASSESSMENT PROCEDURE: PE-8 Assessment Objective	anization review the visitor access logs in accordance with organization-defined frequency. al protection policy; procedures addressing facility access records; information system security plan; facility access doubted out and reviewed by management monthly. References: ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8	Related Controls:
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close Applicability: All ASSESSMENT PROCEDURE: PE-8 Assessment Objective Determine if the organization meets 	anization review the visitor access logs in accordance with organization-defined frequency. a protection policy; procedures addressing facility access records; information system security plan; facility access records; information security plan; facility access records; info	Related Controls:
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close Applicability: All ASSESSMENT PROCEDURE: PE-8 Assessment Objective Determine if the organization meets Assessment Methods And Objects Examine: Physical and environment 	anization review the visitor access logs in accordance with organization-defined frequency. a protection policy; procedures addressing facility access records; information system security plan; facility access records; information security plan; facility access records; info	Related Controls:
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close Applicability: All Assessment Objective Determine if the organization meets Assessment Methods And Objects Examine: Physical and environment access records); facility access control 	anization review the visitor access logs in accordance with organization-defined frequency. a protection policy; procedures addressing facility access records; information system security plan; facility access ad out and reviewed by management monthly. References: ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8 (0).1 the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this ar a protection policy; procedures addressing facility access records; information system security plan (for organization)	Related Controls:
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close Applicability: All Assessment Objective Determine if the organization meets Assessment Methods And Objects Examine: Physical and environment access records); facility access contr PE-8(1) – Enhancement (High) 	anization review the visitor access logs in accordance with organization-defined frequency. a protection policy; procedures addressing facility access records; information system security plan; facility access ad out and reviewed by management monthly. References: ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8 (0).1 the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this ar a protection policy; procedures addressing facility access records; information system security plan (for organization)	Related Controls:
 time of entry and departure; purpose of visit; name and organization of person vi (iii) designated officials within the org Assessment Methods And Objects Examine: Physical and environment records. PE-8(0) – Enhancement (High) Control Visitor access records must be close Applicability: All Assessment Objective Determine if the organization meets Assessment Methods And Objects Examine: Physical and environment access records); facility access control PE-8(1) – Enhancement (High) Control 	anization review the visitor access logs in accordance with organization-defined frequency. a protection policy; procedures addressing facility access records; information system security plan; facility access ad out and reviewed by management monthly. References: ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8 (0).1 the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this ar a protection policy; procedures addressing facility access records; information system security plan (for organization)	Related Controls:

ASSESSMENT PROCEDURE: PE-8(1).1	
Assessment Objective	
Determine if the organization employs automated mechanisms to facilitate the maintenance and review of access records.	
Assessment Methods And Objects	
Examine: Physical and environmental protection policy; procedures addressing facility access records; automated mechanisms supporting management	of access records: facility access control logs
or records; other relevant documents or records.	
PE-8(2) – Enhancement (High)	
Control	
Maintain records of all physical access, both visitor and authorized individuals.	
Applicability: All References: ARS: PE-8(2); NIST 800-53/53A: PE-8(2)	Related Controls:
ASSESSMENT PROCEDURE: PE-8(2).1	Related Controls.
Assessment Objective	
Determine if the organization maintains a record of all physical access, both visitor and authorized individuals.	
Assessment Methods And Objects Examine: Physical and environmental protection policy; procedures addressing facility access records; facility access control logs or records; other relevant	ant degumente er regerde
PE-9 – Power Equipment and Power Cabling (High)	ant documents of records.
Control	
Power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain	safe power for CMS information systems.
Guidance	
Both primary and backup power systems should be included in the safe power implementation procedures. Remote backup site's power implementation	
Applicability: All References: ARS: PE-9; NIST 800-53/53A: PE-9; PISP: 4.11.9	Related Controls:
ASSESSMENT PROCEDURE: PE-9.1	
Assessment Objective	
Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.	
Assessment Methods And Objects	
Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipmer	nt and cabling; other relevant documents or
records.	
PE-9(1) – Enhancement (High)	
Control	
Employ redundant and parallel power cabling paths.	
Applicability: All References: ARS: PE-9(1); NIST 800-53/53A: PE-9(1)	Related Controls:
ASSESSMENT PROCEDURE: PE-9(1).1	
Assessment Objective	
Determine if the organization employs redundant and parallel power cabling paths.	
Assessment Methods And Objects	
Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipmer	nt and cabling; other relevant documents or
records.(Optional)	
PE-9(CMS-1) – Enhancement (High)	
Control	
Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.	
Applicability: All References: ARS: PE-9(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: PE-9(CMS-1).1	
Assessment Objective	
Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.	
Determine if the eigenization prototo power equipment and power easing for the information system for damage and desired lot.	

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets. Interview: Organizational personnel with physical access control responsibilities to determine if only authorized maintenance personnel are permitted to access, including power generators, HVAC systems, cabling, and wiring closets.

generatore, invite eyeteme, eability, and ming		
PE-9(CMS-2) – Enhancement (High)		
Control		
Power surge protection must be implemented for		
Applicability: All	References: ARS: PE-9(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: PE-9(CMS-2).1		
Assessment Objective		
Determine if the organization protects power equ	ipment and implements surge protection for all computers to assist in protection from damage or destruct	tion.
Assessment Methods And Objects		
	n policy; procedures addressing power equipment and cabling protection; facility housing power equipme	nt and cabling; other relevant documents
	protection is implemented for all computer equipment.	
	al access control responsibilities to determine if power surge protection is implemented for all computer e	quipment.
	if power surge protection is implemented for all computer equipment.	
PE-10 – Emergency Shutoff (High)		
Control		
	documented, and implemented effectively to provide the capability of shutting off power to any informati	
	hreatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the e	quipment.
Guidance		
	n system resources may include, for example, data centers, server rooms, and mainframe rooms. References: ARS: PE-10: NIST 800-53/53A: PE-10: PISP: 4.11.10	Deleted Controlo
	References: ARS: PE-10; NIST 800-53/53A: PE-10; PISP: 4.11.10	Related Controls:
ASSESSMENT PROCEDURE: PE-10.1		
Assessment Objective		
Determine if:	within a facility containing concentrations of information system recourses (a.g., data contars, converter	ma mainframa raama), and
	within a facility containing concentrations of information system resources (e.g., data centers, server roc ns within a facility containing concentrations of information system resources, the capability of shutting of	
	t endangering personnel by requiring them to approach the equipment.	power to any information system component
Assessment Methods And Objects		
	n policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switche	s: other relevant documents or records.
PE-10(1) – Enhancement (High)		
Control		
	ergency power-off capability from accidental and intentional / unauthorized activation.	
Applicability: All	References: ARS: PE-10(1); NIST 800-53/53A: PE-10(1)	Related Controls:
ASSESSMENT PROCEDURE: PE-10(1).1		,
Assessment Objective		
	ency power-off capability from accidental or unauthorized activation.	
Assessment Methods And Objects		
	n policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switche	s: other relevant documents or records.
PE-10(CMS-1) – Enhancement (High)		
Control		
	pr emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and	I mainframe rooms.
Applicability: All	References: ARS: PE-10(CMS-1)	Related Controls:

ASSESSMENT PROCEDURE: PE-10(CMS-1).1 Assessment Objective Determine if the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment. Assessment Methods And Objects Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms. Interview: Organizational personnel with physical access control responsibilities to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms. Test: Verify by physical inspection to determine if a master power switch or emergency cut-off switch, prominently marked and protected by a cover, is implemented and maintained for data centers, servers, and mainframe rooms. PE-11 – Emergency Power (High) Control Emergency power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to facilitate an orderly shutdown of the CMS information system in the event of a primary power source loss. Guidance Both primary and backup processing locations should be included in the safe power implementation procedures. The remote backup site's power implementation should be included in the documentation. Even though unlikely that both the primary and backup locations will be switching to emergency power at the same time, it is prudent to minimize the risk to a total lose of a processing capability. Applicability: All References: ARS: PE-11; FISCAM: TSC-2.2.5; NIST 800-53/53A: PE-11; PISP: 4.11.11 **Related Controls: ASSESSMENT PROCEDURE: PE-11.1 Assessment Objective** Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. **Assessment Methods And Objects** Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records. Test: Uninterruptible power supply. PE-11(1) – Enhancement (High) Control Provide a long-term alternate power supply for the system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source References: ARS: PE-11(1): NIST 800-53/53A: PE-11(1) Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: PE-11(1).1 Assessment Objective Determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source. **Assessment Methods And Objects** Examine: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records. Test: Alternate power supply. PE-12 – Emergency Lighting (High) Control Mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enhance safety and availability. Automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes shall be provided. Guidance Local building safety codes are a good place to obtain the needed information for documenting emergency lighting implementation procedures and architecture. Applicability: All References: ARS: PE-12; NIST 800-53/53A: PE-12; PISP: 4.11.12 **Related Controls:**

ASSESSMENT PROCEDURE: PE-12.1		
Assessment Objective		
Determine if:		
(i) the organization employs and maintai	ns automatic emergency lighting systems that activates in the event of a power outage or disruption; and	
(ii) the organization employs and mainta	ins automatic emergency lighting systems that cover emergency exits and evacuation routes.	
Assessment Methods And Objects		
	rotection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency ligh	ting test records; emergency exits and
evacuation routes; other relevant docum	ents or records.	
Test: Emergency lighting capability.		
PE-13 – Fire Protection (High)		
Control		
detection devices / systems that can be	place and supporting procedures shall be developed, documented, and implemented effectively to prevent, detect activated in the event of a fire shall be employed and maintained. Fire suppression and detection devices / syst hishers, fixed fire hoses, and smoke detectors.	
Guidance		
	systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smol	ke detectors.
Applicability: All	References: ARS: PE-13; FISCAM: TSC-2.2.1, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-13;	Related Controls:
, ppnoubility i a	PISP: 4.11.13	
ASSESSMENT PROCEDURE: PE-13.1		•
Assessment Objective		
-	nd maintains fire suppression and detection devices/systems that can be activated in the event of a fire.	
Assessment Methods And Objects		
	rotection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire sup	pression and detection devices/systems
documentation; test records of fire suppl	ression and detection devices/systems; other relevant documents or records.	
PE-13(1) – Enhancement (High)		
Control		
Implement and maintain fire detection de	evices / systems that activate automatically and notify the organization and emergency responders in the event o	of a fire.
Applicability: All	References: ARS: PE-13(1); NIST 800-53/53A: PE-13(1)	Related Controls:
ASSESSMENT PROCEDURE: PE-13(1		-
Assessment Objective	<u>, </u>	
Determine if:		
	n devices/systems that activate automatically; and	
	on devices/systems that notify the organization and emergency responders in the event of a fire.	
Assessment Methods And Objects		
Examine: Physical and environmental p	rotection policy; procedures addressing fire protection; facility housing the information system; alarm service lev	vel agreements; test records of fire suppression
and detection devices/systems; fire supp	pression and detection devices/systems documentation; other relevant documents or records.	C
Test: Simulated fire detection and auton	nated notifications.	
PE-13(2) – Enhancement (High)		
Control		
	ns that provide automatic notification of any activation to the organization and emergency responders.	
Applicability: All	References: ARS: PE-13(2); NIST 800-53/53A: PE-13(2)	Related Controls:
ASSESSMENT PROCEDURE: PE-13(2).1	
Assessment Objective		
•	re suppression devices/systems that provide automatic notification of any activation to the organization and eme	ergency responders.
Assessment Methods And Objects		
-	rotection policy; procedures addressing fire protection; fire suppression and detection devices/systems docume	ntation: facility housing the information system:
	1 - 2/1	,,

	cords of fire suppression and detection devices/systems; other relevant documents or records ession devices/systems and automated notifications.	ords.
PE-13(3) – Enhancement (High)		
Control		
Employ an automatic fire suppression c	apability in facilities that are not staffed on a continuous basis.	
Applicability: All	References: ARS: PE-13(3); NIST 800-53/53A: PE-13(3)	Related Controls:
ASSESSMENT PROCEDURE: PE-13(3	3).1	
Assessment Objective		
Determine if the organization employs a	n automatic fire suppression capability in facilities that are not staffed on a continuous ba	sis.
ssessment Methods And Objects		
Examine: Physical and environmental p	protection policy; procedures addressing fire protection; facility housing the information sy	stem; alarm service level agreements; facility staffing plans; test
	n devices/systems; other relevant documents or records.	
	ession devices/systems and automated notifications.	
PE-14 – Temperature and Humidit	ty Controls (High)	
Control		
	nanisms shall be in place and supporting procedures shall be developed, documented, an f facilities containing CMS information systems.	d implemented effectively to maintain (within acceptable levels) and
Guidance		
Local building a safety codes are a good Health Administration (OSHA) requirem	d place to obtain the needed information for documenting HVAC implementation procedur ents maybe included.	es and architecture. Consideration for Occupational Safety and
Applicability: All	References: ARS: PE-14; FISCAM: TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: I	PE-14; PISP: 4.11.14 Related Controls:
SSESSMENT PROCEDURE: PE-14.1		•
(ii) the organization regularly monitors the ssessment Methods And Objects Examine: Physical and environmental preserved.	within acceptable levels, the temperature and humidity within the facility where the inform ne temperature and humidity within the facility where the information system resides. protection policy; procedures addressing temperature and humidity control; facility housing mentation; temperature and humidity records; other relevant documents or records.	
PE-14(CMS-1) – Enhancement (High)	······································	
Control		
Evaluate the level of alert and follow pre	escribed guidelines for that alert level	
Applicability: All	References: ARS: PE-14(CMS-1)	Related Controls:
SSESSMENT PROCEDURE: PE-14(0		
ssessment Objective		
Determine if:		
	within acceptable levels, the temperature and humidity within the facility where the inform	ation system resides: and
	he temperature and humidity within the facility where the information system resides.	······································
ssessment Methods And Objects		
Examine: Physical and environmental p temperature and humidity controls docu	protection policy; procedures addressing temperature and humidity control; facility housing mentation; temperature and humidity records; other relevant documents or records to det	ermine the level of alert and prescribed guidelines for that alert leve
	h environmental protection responsibilities to determine if there exists the level of alert an	
PE-14(CMS-2) – Enhancement (High)		
Control		
Alert component management of possib		
Applicability: All	References: ARS: PE-14(CMS-2)	Related Controls:
Rev. 9	Page 130 of 207	BPSSM Appendix A, Attachment

ASSESSMENT PROCEDURE: PE-14(CMS-2)	.1	
Assessment Objective		
	management personnel of loss of service or media.	
Assessment Methods And Objects		
	n policy; procedures addressing temperature and humidity control; facility housing the information system	m: temperature and humidity controls:
	on; temperature and humidity records; other relevant documents or records to determine an alert is gene	
loss of service and/or media.		
	nmental protection responsibilities to determine an alert is generated to component management of pos	sible loss of service and/or media.
PE-14(CMS-3) – Enhancement (High)		
Control		
Report damage and provide remedial action. In		
Applicability: All	References: ARS: PE-14(CMS-3)	Related Controls:
ASSESSMENT PROCEDURE: PE-14(CMS-3)	.1	
Assessment Objective		
Determine if the organization regularly monitors	the temperature and humidity within the facility where the information system resides.	
Assessment Methods And Objects		
	n policy; procedures addressing temperature and humidity control; facility housing the information system	
, ,	on; temperature and humidity records; other relevant documents or records to determine damage is repo	orted and remedial action is taken, including the
implementation of contingency plan.		
	nmental protection responsibilities to determine to determine if damage is reported and remedial action	is taken, including the implementation of
contingency plan. PE-14(FIS-1) – Enhancement (High)		
Control		
Redundancy exists in the air cooling system.		
	References: FISCAM: TSC-2.2.3	Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1		Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective		Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai		Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects		Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities.	r cooling systems.	Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an	r cooling systems.	Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures.	r cooling systems.	Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager.	r cooling systems. d access to the air cooling systems.	Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures.	r cooling systems. d access to the air cooling systems.	Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (Hig Control	r cooling systems. d access to the air cooling systems. h)	
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (Hig Control	r cooling systems. d access to the air cooling systems. h) at the building plumbing does not endanger CMS information systems. Procedures shall be developed, d	
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (High Control All necessary steps shall be taken to ensure tha	r cooling systems. d access to the air cooling systems. h) at the building plumbing does not endanger CMS information systems. Procedures shall be developed, d	
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (Hig Control All necessary steps shall be taken to ensure tha reduce the potential damage from plumbing leal Guidance Local building a safety codes are a good place t	r cooling systems. d access to the air cooling systems. h) at the building plumbing does not endanger CMS information systems. Procedures shall be developed, d ks.	locumented, and implemented effectively to
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (Hig Control All necessary steps shall be taken to ensure tha reduce the potential damage from plumbing leaf Guidance	r cooling systems. d access to the air cooling systems. h) At the building plumbing does not endanger CMS information systems. Procedures shall be developed, d ks. to obtain the needed information for documenting water damage protection procedures and architecture. ybe included. References: ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15;	locumented, and implemented effectively to
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (Hig Control All necessary steps shall be taken to ensure tha reduce the potential damage from plumbing leal Guidance Local building a safety codes are a good place t Health Administration (OSHA) requirements ma	r cooling systems. d access to the air cooling systems. h) at the building plumbing does not endanger CMS information systems. Procedures shall be developed, d ks. to obtain the needed information for documenting water damage protection procedures and architecture. ybe included.	locumented, and implemented effectively to
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (Hig Control All necessary steps shall be taken to ensure tha reduce the potential damage from plumbing lead Guidance Local building a safety codes are a good place t Health Administration (OSHA) requirements ma Applicability: All ASSESSMENT PROCEDURE: PE-15.1	r cooling systems. d access to the air cooling systems. h) At the building plumbing does not endanger CMS information systems. Procedures shall be developed, d ks. to obtain the needed information for documenting water damage protection procedures and architecture. ybe included. References: ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15;	locumented, and implemented effectively to
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (Hig Control All necessary steps shall be taken to ensure tha reduce the potential damage from plumbing leaf Guidance Local building a safety codes are a good place t Health Administration (OSHA) requirements ma Applicability: All ASSESSMENT PROCEDURE: PE-15.1 Assessment Objective	r cooling systems. d access to the air cooling systems. h) At the building plumbing does not endanger CMS information systems. Procedures shall be developed, d ks. to obtain the needed information for documenting water damage protection procedures and architecture. ybe included. References: ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15;	locumented, and implemented effectively to
ASSESSMENT PROCEDURE: PE-14(FIS-1).1 Assessment Objective Determine if the organization uses redundant ai Assessment Methods And Objects Examine: Entity's facilities. Examine: Operation, location, maintenance, an Examine: Pertinent policies and procedures. Interview: Site manager. PE-15 – Water Damage Protection (Hig Control All necessary steps shall be taken to ensure tha reduce the potential damage from plumbing leal Guidance Local building a safety codes are a good place t Health Administration (OSHA) requirements ma Applicability: All ASSESSMENT PROCEDURE: PE-15.1 Assessment Objective Determine if:	r cooling systems. d access to the air cooling systems. h) At the building plumbing does not endanger CMS information systems. Procedures shall be developed, d ks. to obtain the needed information for documenting water damage protection procedures and architecture. ybe included. References: ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15;	locumented, and implemented effectively to . Consideration for Occupational Safety and Related Controls:

(ii) the organization protects the information system from water damage resulting from broken plumbing lines or other sources of v working properly, and known to key personnel.	vater leakage by providing master shutoff valves that are accessible,
Assessment Methods And Objects	
Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the info knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value documer Interview: Organization personnel with physical and environmental protection responsibilities.	
Test: Simulated master water shutoff value activation for the plumbing system.	
PE-15(1) – Enhancement (High)	
Control	
Mechanisms are employed that, without the need for manual intervention, protect the information system from water damage in th	
Applicability: All References: ARS: PE-15(1); NIST 800-53/53A: PE-15(1)	Related Controls:
ASSESSMENT PROCEDURE: PE-15(1).1	
Assessment Objective	
Determine if the organization employs mechanisms that, without the need for manual intervention, protect the information system	from water damage in the event of a significant water leak.
Assessment Methods And Objects	
Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the info other relevant documents or records.	rmation system; automated mechanisms for water shutoff valves;
Test: Automated mechanisms implementing master water shutoff valve activation.	
PE-16 – Delivery and Removal (High)	
Control	
Procedures shall be developed, documented, and implemented effectively to control the flow of information system-related items i the delivery or removal of CMS information system-related items. To avoid unauthorized access, delivery and removal controls shall be implemented to isolate delivery areas from sensitive facilitie	
information systems, and media libraries.	
Guidance	
The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avo	
Applicability: All References: ARS: PE-16; NIST 800-53/53A: PE-16; PISP: 4.11.16	Related Controls:
ASSESSMENT PROCEDURE: PE-16.1	
Assessment Objective	
Determine if:	
 (i) the organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility; a (ii) the organization maintains appropriate records of items entering and exiting the facility. 	nd
Assessment Methods And Objects	
Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system comp	opents from the facility: facility housing the information system:
records of items entering and exiting the facility; other relevant documents or records.	onents norm the facility, facility housing the information system,
Interview: Organization personnel with tracking responsibilities for information system components entering and exiting the facility	Ι.
PE-17 – Alternate Work Site (High)	
Control	
Procedures shall be developed, documented, and implemented effectively to control information system security at alternate work at alternate work sites to report security issues or suspected security incidents.	sites. A method of communication shall be provided to employees
Guidance	
The organization provides a means for employees to communicate with information system security staff in case of security proble	ems. NIST SP 800-46 provides guidance on security in
telecommuting and broadband communications	
telecommuting and broadband communications. Applicability: All References: ARS: PE-17; HIPAA: 164.310(a)(2)(i); NIST 800-53/53A: PE-17; P	SP: 4.11.17 Related Controls:

ASSESSMENT PROCEDURE: PE-17.1				
Assessment Objective				
Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.				
Assessment Methods And Objects				
	policy; procedures addressing alternate work sites for organizational personnel; list of management, op	erational, and technical security controls		
required for alternate work sites; other relevant of				
Interview: Organization personnel using alterna	te work sites.			
PE-17(CMS-1) – Enhancement (High)				
Control				
about laptops, and disconnecting modems when	work sites. Security controls may include, but are not limited to, laptop cable locks, recording serial nun	nbers and other identification information		
Applicability: All	References: ARS: PE-17(CMS-1)	Related Controls:		
ASSESSMENT PROCEDURE: PE-17(CMS-1).				
Assessment Objective	·			
-	te management, operational, and technical information system security controls at alternate work sites.			
Assessment Methods And Objects				
	policy; procedures addressing alternate work sites for organizational personnel; list of management, op	erational, and technical security controls		
required for alternate work sites; other relevant of	ocuments or records to determine if appropriate security controls at alternate work sites are employed.			
	mbers and other identification information about laptops, and disconnecting modems when not in use.			
	te worksite responsibilities to determine if appropriate security controls at alternate work sites are employ			
	I numbers and other identification information about laptops, and disconnecting modems when not in use			
PE-18 – Location of Information System	Components (High)			
Control				
Procedures shall be developed, documented, and and environmental hazards, and to minimize the	d implemented effectively to ensure that information system components are positioned within the facility	y to minimize potential damage from physical		
Guidance				
	example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interfe	rence, and electromagnetic radiation		
	lers the location or site of the facility with regard to physical and environmental hazards.	rence, and electromagnetic radiation.		
Applicability: All	References: ARS: PE-18; FISCAM: TAN-2.1.1, TAN-2.1.2; HIPAA: 164.312(c)(1); NIST 800-53/53A:	Related Controls:		
	PE-18; PISP: 4.11.18			
ASSESSMENT PROCEDURE: PE-18.1				
Assessment Objective				
Determine if:				
	components within the facility to minimize potential damage from physical and environmental hazards; a	nd		
	components within the facility to minimize the opportunity for unauthorized access.			
Assessment Methods And Objects	a policy procedures addressing positioning of information system components, documentation providing	the leastion and position of information		
system components within the facility: other rele	 policy; procedures addressing positioning of information system components; documentation providing vant documents or records 	the location and position of information		
system components within the facility; other relevant documents or records. PE-18(1) – Enhancement (High)				
Control				
	cilities with regard to physical and environmental bazards and, for existing facilities, consider the physica	l and environmental bazards in the risk		
Plan the location or site of information system facilities with regard to physical and environmental hazards and, for existing facilities, consider the physical and environmental hazards in the risk mitigation strategy.				
Applicability: All	References: ARS: PE-18(1); NIST 800-53/53A: PE-18(1)	Related Controls:		
ASSESSMENT PROCEDURE: PE-18(1).1				
Assessment Objective				
Determine if:				
(i) the organization plans the location or site of the	he facility where the information system resides with regard to physical and environmental hazards; and			
Rev. 9	Page 133 of 207	BPSSM Appendix A, Attachment 1		

(ii) the organization, for existing facili	(ii) the organization, for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.		
Assessment Methods And Objects			
	al protection policy; physical site planning documents; organizational assessment of risk, continge ith site selection responsibilities for the facility housing the information system.	ency plan; other relevant documents or records.	
PE-19 – Information Leakage (C	ptional) (High)		
Control			
Safeguards and countermeasures sh	ould be considered to protect information systems against information leakage due to electromage	gnetic signals emanations.	
Guidance			
	 (for confidentiality) of the information system and organizational security policy guides the applic nation leakage due to electromagnetic signals emanations. 	ation of safeguards and countermeasures employed to protect	
Applicability: Optional for all	References: ARS: PE-19; NIST 800-53/53A: PE-19; PISP: 4.11.19	Related Controls:	
ASSESSMENT PROCEDURE: PE-1	9.1		
Assessment Objective			
Determine if the organization protect	s the information system from information leakage due to electromagnetic signals emanations.		
Assessment Methods And Objects			
against electronic signals emanation	al protection policy; procedures addressing information leakage due to electromagnetic signals en facility housing the information system; records from electromagnetic signals emanation tests; o tion leakage due to electromagnetic signals emanations.(Optional)		

Planning (PL) – Management

PL-1 – Security Planning Policy and Procedures (High)

Control

All CMS information systems and major applications shall be documented in a SSP, which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, in accordance with current CMS Procedures.

Guidance

The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-18 provides guidance on security planning. NIST SP 800-12 provides guidance on security policies and procedures.

ASSESSMENT PROCEDURE: PL-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security planning policy and procedures;

(ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review security planning policy and procedures; and

(iv) the organization updates security planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system security planning and plan implementation responsibilities.

ASSESSMENT PROCEDURE: PL-1.2

Assessment Objective

Determine if:

(i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system security planning and plan implementation responsibilities.

References: FISCAM: TSP-3.3.2

PL-1(FIS-1) – Enhancement (High)

Control

Security policies are distributed to all affected personnel.

Applicability: All

ASSESSMENT PROCEDURE: PL-1(FIS-1).1

Assessment Objective

Determine if the organization distributes security policies to all affected personnel.

Assessment Methods And Objects

Examine: Memos, electronic mail files, or other policy distribution mechanisms.

Interview: Staff and system users to determine how security policies are distributed.

PL-2 – System Security Plan (SSP) (High)

Control

All CMS information systems and major applications shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18. The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization

Related Controls:

	sources management strategic plan. The information contained in the SSP is subject to reporting require s, standards, and guidance, including, but not limited to, current CMS Procedures.	ments as established by applicable laws,
Guidance		
The security plan is aligned with the organizatior	s' information system architecture and information security architecture. NIST SP 800-18 provides guida	nce on security planning.
Applicability: All	References: ARS: PL-2; FISCAM: TAC-3.1.A.1, TSP-2.1, TSP-3.2; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3; NIST 800-53/53A: PL-2; PISP: 4.12.2	Related Controls:
ASSESSMENT PROCEDURE: PL-2.1		
Assessment Objective		
(iii) the security plan development is consistent v and supplementation of the tailored baseline;	security requirements for the information system and a description of the security controls planned or in vith NIST SP 800-18 and the concepts in the NIST Risk Management Framework including baseline security architecture; and ization's information system architecture and information security architecture; and	
	addressing information system security plan development and implementation; NIST SP 800-18; security	plan for the information system; other
relevant documents or records.	ation system assurity planning and plan implementation responsibilities	
PL-2(CMS-1) – Enhancement (High)	ation system security planning and plan implementation responsibilities.	
Control	stem according to the CMS System Security Plan (SSP) Procedures.	
Applicability: All	References: ARS: PL-2(CMS-1); FISCAM: TSP-2.1; HIPAA: 164.316(b)(1)(i), 164.316(b)(1)(ii); HSPD	Related Controls:
	7: J(35); IRS-1075: 4.7.3#2	Nelated Controls.
ASSESSMENT PROCEDURE: PL-2(CMS-1).1		
(iii) the security plan is consistent with NIST SP ((iv) the security plan is consistent with the organ	security requirements for the information system and a description of the security controls planned or in 300-18; ization's information system architecture and information security architecture; and	place for meeting the security requirements;
(v) designated organizational officials review and Assessment Methods And Objects	approve the security plan.	
Examine: Security planning policy; procedures a relevant documents or records to determine the Interview: Organizational personnel with inform controls of the system and are documented according to the system and are documented according to the system and the s	addressing information system security plan development and implementation; NIST SP 800-18; security in-place security controls of the system are documented according to the CMS System Security Plan (SS ation system security planning and plan implementation responsibilities to determine if System Security F ording to the CMS System Security Plan (SSP) Procedures.	SP) Procedures.
PL-2(PII-1) – Enhancement (High)		
Control Make documentation available to those persons	responsible for implementing the procedures to which the documentation pertains.	
Applicability: All	References: HIPAA: 164.316(b)(2)(ii)	Related Controls:
ASSESSMENT PROCEDURE: PL-2(PII-1).1		·
Assessment Objective Determine if the organization provides to those p Assessment Methods And Objects Examine: Procedures that document who obtain	persons responsible for implementing the procedures to which the documentation pertains. In a documentation and which documentation pertains to whom for implementation. Sponsible for implementation of procedures to determine if documentation is available.	
Rev. 9	Page 136 of 207	BPSSM Appendix A, Attachment 1

PL 2(UIP 1) Enhancement (High)			
PL-2(HIP-1) – Enhancement (High)			
Control Retain documentation of policies and procedures relating to HIPAA 164.306 for 6 years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)			
	References: HIPAA 164.316(b)(2)(i)	Related Controls:	
Applicability: All ASSESSMENT PROCEDURE: PL-2(HIP-1).1	References: HIPAA. 164.316(0)(2)(1)	Related Controls:	
Assessment Objective		to sub-section and the strength of the strength between the between	
(See HIPAA 164.316(b))	tion of policies and procedures relating to 164.306 for six (6) years from the date of its creation or the da	te when it last was in effect, whichever is later.	
Assessment Methods And Objects			
-	ies and procedures relating to 164.306 is held for six (6) years from the date of its creation or the date whet	nen it last was in effect, whichever is later.	
(See HIPAA 164.316(b))		·	
	if documentation of policies and procedures relating to 164.306 is held for six (6) years from the date of	its creation or the date when it last was in	
effect, whichever is later. (See HIPAA 164.316(b			
PL-2(IRS-1) – Enhancement (High)			
Control			
	e, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition to those specified in ot		
Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS	References: IRS-1075: 5.6.3.5#3	Related Controls:	
ASSESSMENT PROCEDURE: PL-2(IRS-1).1			
Assessment Objective			
	nto a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition t	to those specified in other controls	
Assessment Methods And Objects			
	h IRS Pub 1075 Exhibit 7 while FTI is incorporated into a Data Warehouse.		
PL-2(IRS-2) – Enhancement (High)			
PL-2(IRS-2) – Enhancement (High) Control		the confidentiality of the information received	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce from the IRS. Annually thereafter, the organizat	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce	edures or safeguards described in the SPR. It	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures, summarizes the organization's current efforts to ensure the	edures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan	edures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub.	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8)	dures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC,	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan	edures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies	
 PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS 	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8)	dures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8)	dures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1	dures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the o thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the o thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir future actions that will affect the organization's safeguard procedures, summarizes the organization's cur	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of	
 PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Procee from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is 	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the o thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir future actions that will affect the organization's safeguard procedures, summarizes the organization's cur protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Wh	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of	
 PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Procee from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is safeguard program the SPR will be updated and 	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the o thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir future actions that will affect the organization's safeguard procedures, summarizes the organization's cur	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of	
 PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Procee from the IRS. Annually thereafter, the organizati also advises the IRS of future actions that will af that the organization is protecting FTI pursuant twill be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and submit the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is safeguard program the SPR will be updated and Assessment Methods And Objects 	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the o thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir future actions that will affect the organization's safeguard procedures, summarizes the organization's cur protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Wh resubmitted. (See IRS Pub. 1075, sections 7 & 8).	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of	
 PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is safeguard program the SPR will be updated and Assessment Methods And Objects Examine: Safeguard Procedure Reports to determine 	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the o thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir future actions that will affect the organization's safeguard procedures, summarizes the organization's cu protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Wh d resubmitted. (See IRS Pub. 1075, sections 7 & 8).	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of	
 PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Procee from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is safeguard program the SPR will be updated and Assessment Methods And Objects Examine: Safeguard Procedure Reports to determine 	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedifect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization's current file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir future actions that will affect the organization's safeguard procedures, summarizes the organization's current file a Safeguard procedures, summarizes the organization's current future actions that will affect the organization's safeguard procedures, summarizes the organization's current future actions that will affect the organization's safeguard procedures, summarizes the organization's current future actions that will affect and used ensure confidentially of the FTI data received from the IRS. ine annual submission and protections are in accordance with the Safeguard Procedure Report.	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of	
 PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is safeguard program the SPR will be updated and Assessment Methods And Objects Examine: Safeguard Procedure Reports to determine PL-3 – System Security Plan Update (H 	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedifect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization's current file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir future actions that will affect the organization's safeguard procedures, summarizes the organization's current file a Safeguard procedures, summarizes the organization's current future actions that will affect the organization's safeguard procedures, summarizes the organization's current future actions that will affect the organization's safeguard procedures, summarizes the organization's current future actions that will affect and used ensure confidentially of the FTI data received from the IRS. ine annual submission and protections are in accordance with the Safeguard Procedure Report.	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is safeguard program the SPR will be updated and Assessment Methods And Objects Examine: Safeguard Procedure Reports to determine Examine: Safeguard Activity Reports to determine PL-3 – System Security Plan Update (H Control	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the proce fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the io IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the o thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of min future actions that will affect the organization's safeguard procedures, summarizes the organization's current so protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenevers. Whenevers. Whenevers armine the procedures established and used ensure confidentially of the FTI data received from the IRS. ine annual submission and protections are in accordance with the Safeguard Procedure Report. igh)	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of enever significant changes occur in the	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is safeguard program the SPR will be updated and Assessment Methods And Objects Examine: Safeguard Activity Reports to determine PL-3 – System Security Plan Update (H Control The SSP shall be reviewed at least every 365 dat	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedifect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization's current file a Safeguard Activity Report (SAR). The SAR advises the IRS of mir future actions that will affect the organization's safeguard procedures, summarizes the organization's current file a Safeguard procedures, summarizes the organization's current future actions that will affect the organization's safeguard procedures, summarizes the organization's current future actions that will affect the organization's safeguard procedures, summarizes the organization's current future actions that will affect and used ensure confidentially of the FTI data received from the IRS. ine annual submission and protections are in accordance with the Safeguard Procedure Report.	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of enever significant changes occur in the ficant changes made to the information	
PL-2(IRS-2) – Enhancement (High) Control For FTI, develop and submit a Safeguard Proce- from the IRS. Annually thereafter, the organizat also advises the IRS of future actions that will af that the organization is protecting FTI pursuant t will be updated and resubmitted. (See IRS Pub. Applicability: All; Optional for ABMAC, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, SS ASSESSMENT PROCEDURE: PL-2(IRS-2).1 Assessment Objective Determine if the organization develops and subr the information received from the IRS. Annually described in the SPR. It also advises the IRS of FTI, and finally, certifies that the organization is safeguard program the SPR will be updated and Assessment Methods And Objects Examine: Safeguard Activity Reports to determine PL-3 – System Security Plan Update (H Control The SSP shall be reviewed at least every 365 dat	dures Report (SPR) that describes the procedures established and used by the organization for ensuring ion must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures fect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant chan 1075, sections 7 & 8) References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1 mits a Safeguard Procedures Report (SPR) that describes the procedures established and used by the o thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of min future actions that will affect the organization's safeguard procedures, summarizes the organization's current for the regulation to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever the organization is a safeguard procedure, summarizes the organization's current future actions that will affect the organization for ensure the organization's own security requirements. Whenever the organization is a safeguard procedure, summarizes the organization's current to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever the procedures established and used ensure confidentially of the FTI data received from the IRS. ine annual submission and protections are in accordance with the Safeguard Procedure Report. igh) ays and updated minimally every three (3) years to reflect current conditions or whenever there are significant current conditions or whenever there are significant current conditions or whenever there are significant enterprice and the organization or whenever there are significant enterprice and the organization is or whenever there are significant enterprice.	Adures or safeguards described in the SPR. It e confidentiality of FTI, and finally, certifies ges occur in the safeguard program the SPR Related Controls: rganization for ensuring the confidentiality of nor changes to the procedures or safeguards rrent efforts to ensure the confidentiality of enever significant changes occur in the ficant changes made to the information	

Guidance Significant changes are defined in advance by the organization and identified in the configuration management process. NIST SP 800-18 provides guidance on security plan updates. Applicability: All References: ARS: PL-3: FISCAM: TSP-2,2: HIPAA: 164,306(a)(3), 164,316(a), 164,316(b)(2)(iji): **Related Controls:** HSPD 7: G(24), J(35); IRS-1075: 5.6.1.2#1.4; NIST 800-53/53A: PL-3; PISP: 4.12.3 **ASSESSMENT PROCEDURE: PL-3.1 Assessment Objective** Determine if: (i) the organization defines the frequency of information system security plan reviews and updates; (ii) the organization updates the security plan in accordance with organization-defined frequency, at least annually: (iii) the organization receives input to update the security plan from the organization's configuration management and control process; and (iv) the updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls. **Assessment Methods And Objects** Examine: Security planning policy: procedures addressing information system security plan updates; information system security plan; configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records. PL-4 – Rules of Behavior (ROB) (High) Control ROBs shall be established, and made readily available, to delineate clearly user responsibilities and expected behavior of all Business Owners, users, operators, and administrators with regard to information and information system usage. Before authorizing access to the information system and / or information and annually thereafter, the organization shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the ROBs. Specific ROBs shall be established to govern work-at-home users who access CMS information or information systems. Limited personal use of organization-owned or leased equipment and resources shall be considered to be a permitted use of organization-owned or leased equipment and resources when the following conditions are met: 4.12.4.1. Such use involves minimal additional expense to CMS; 4.12.4.2. Such use does not interfere with the mission or operation of CMS: 4.12.4.3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch: 4.12.4.4. Such use does not overburden any CMS information system resources; 4.12.4.5. Such use is not otherwise prohibited under this policy; and 4.12.4.6. Any use of organizational Internet and email resources shall be made with the understanding that such use is not secure, private or anonymous. The following uses of organization-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited: 4.12.4.7. Activities that are in violation of law. Government-wide rule or regulation or that are otherwise inappropriate for the workplace: 4.12.4.8. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords; 4.12.4.9. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity; 4.12.4.10. All email communications to groups of employees that are subject to approval prior to distribution and have not been approved by the organization (e.g., retirement announcements, union notices or announcements, charitable solicitations); and 4.12.4.11. Employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees. All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of organization-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that employees desire to protect their privacy, employees shall not use organization-owned or leased equipment and resources. Guidance Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST SP 800-18 provides guidance on preparing rules of behavior. Applicability: All References: ARS: PL-4; FISCAM: TSP-3.3.2; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: **Related Controls:** 5.6.1.2#1.5: NIST 800-53/53A: PL-4: PISP: 4.12.4 **ASSESSMENT PROCEDURE: PL-4.1 Assessment Objective** Determine if:

(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;

() 0	ules available to all information system users;	
.,	anizational personnel are consistent with NIST SP 800-18; and	
., .	signed acknowledgement from users indicating that they have read, understand, and agr	ree to abide by the rules of behavior, before authorizing access to the
information system and its reside		
ssessment Methods And Obj		
, i i i i i i i i i i i i i i i i i i i	icy; procedures addressing rules of behavior for information system users; NIST SP 800- nnel who are authorized users of the information system and have signed rules of behav	
PL-4(CMS-1) – Enhancement (H		
	lign)	
ontrol	the content of a found one.	
Define user roles and expectation	References: ARS: PL-4(CMS-1)	Deleted Controlo
pplicability: All SSESSMENT PROCEDURE: F		Related Controls:
	² -4(CWIS-1).1	
ssessment Objective		
Determine if: (i) the organization establishes a	a set of rules that describe user responsibilities and expected behavior with regard to info	ormation system usage:
., .	ules available to all information system users;	ormation system usage,
., .	anizational personnel are consistent with NIST SP 800-18; and	
()	signed acknowledgement from users indicating that they have read, understand, and agr	ree to abide by the rules of behavior, before authorizing access to the
information system and its reside		
ssessment Methods And Obj	ects	
	icy; procedures for the development and implementation of rules of behavior for informat	tion system users; NIST SP 800-18; rules of behavior; other relevant
	ine user roles and expectations for system and network use are defined.	
	nnel who are authorized users of the information system and have signed rules of behav	vior to determine user roles and expectations for system and network use ar
defined. PL-4(CMS-2) – Enhancement (H		
	ngn)	
Control		
	table as signed acknowledgement of rules-of-behavior (ROB). References: ARS: PL-4(CMS-2)	Deleted Controls
		Related Controls:
SSESSMENT PROCEDURE: F	² L-4(CWIS-2).1	
ssessment Objective		
Determine if:	a set of rules that describe user responsibilities and expected behavior with regard to info	ormation system usage:
., .	ules available to all information system users;	ormation system usage,
., .	anizational personnel are consistent with NIST SP 800-18; and	
.,	signed acknowledgement from users indicating that they have read, understand, and agr	ree to abide by the rules of behavior, before authorizing access to the
information system and its reside		
ssessment Methods And Obj		
	icy; procedures for the development and implementation of rules of behavior for informat ine electronic signatures are acceptable as signed acknowledgement of rules-of-behavio	
Interview: Organizational perso acknowledgement of rules-of-be	nnel who are authorized users of the information system and have signed rules of behave havior (ROB).	vior to determine electronic signatures are acceptable as signed
PL-5 – Privacy Impact Asse		
Control		
	S information systems. The PIAs shall be compliant with the E-Government Act of 2002, s and regulations.	2, OMB Memorandum M-03-22, and the Health Insurance Portability and
Guidance	¥	
	des guidance for implementing the privacy provisions of the E-Government Act of 2002.	
I -		
Day 0	Page 130 of 207	BPSSM Appendix A Attachmen

Applicability: All; Optional for ABMAC, COB, CWF,	References: ARS: PL-5; HSPD 7: J(35); NIST 800-53/53A: PL-5; PISP: 4.12.5	Related Controls:
DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC,		
SS, ZPIC		
ASSESSMENT PROCEDURE: PL-5.1		
Assessment Objective		
Determine if:		
(i) the organization conducts a privacy impact as	sessment on the information system in accordance with OMB policy; and	
(ii) the privacy impact assessment is consistent v	with federal legislation and OMB policy.	
Assessment Methods And Objects		
	addressing privacy impact assessments on the information system; appropriate federal legisla	ation and OMB policy; privacy impact assessment; othe
relevant documents or records.		
PL-6 – Security-Related Activity Plannin	ıg (High)	
Control		
Security-related activities affecting the informatic	on system shall be planned and coordinated before being performed in order to reduce the im	pact on CMS operations (i.e. mission functions image
	si system shall be planned and obordinated before being performed in order to reduce the imp	pact on Civis operations (i.e., mission, functions, image
and reputation), organizational assets, and indivi	iduals. Routine security-related activities include, but are not limited to, security assessments	s, audits, system hardware and software maintenance,
and reputation), organizational assets, and indivises of the security certifications, and testing / exercises.		s, audits, system hardware and software maintenance,
and reputation), organizational assets, and indivisecurity certifications, and testing / exercises. O Guidance	iduals. Routine security-related activities include, but are not limited to, security assessments rganizational advance planning and coordination includes both emergency and non-emergen	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations.
and reputation), organizational assets, and indivi security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are	iduals. Routine security-related activities include, but are not limited to, security assessments rganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations.
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordination	iduals. Routine security-related activities include, but are not limited to, security assessments rganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so on includes both emergency and non-emergency (i.e., routine) situations.	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations. ecurity certifications, and testing/exercises.
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordinatio Applicability: All	iduals. Routine security-related activities include, but are not limited to, security assessments rganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations.
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordination Applicability: All ASSESSMENT PROCEDURE: PL-6.1	iduals. Routine security-related activities include, but are not limited to, security assessments rganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so on includes both emergency and non-emergency (i.e., routine) situations.	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations. ecurity certifications, and testing/exercises.
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but arr Organizational advance planning and coordination Applicability: All ASSESSMENT PROCEDURE: PL-6.1 Assessment Objective	iduals. Routine security-related activities include, but are not limited to, security assessments rganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so on includes both emergency and non-emergency (i.e., routine) situations.	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations. ecurity certifications, and testing/exercises.
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordinatio Applicability: All ASSESSMENT PROCEDURE: PL-6.1 Assessment Objective Determine if:	iduals. Routine security-related activities include, but are not limited to, security assessments irganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so on includes both emergency and non-emergency (i.e., routine) situations. References: ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations. ecurity certifications, and testing/exercises. Related Controls:
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordinatio Applicability: All ASSESSMENT PROCEDURE: PL-6.1 Assessment Objective Determine if: (i) the organization plans and coordinates securi	iduals. Routine security-related activities include, but are not limited to, security assessments rganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so on includes both emergency and non-emergency (i.e., routine) situations.	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations. ecurity certifications, and testing/exercises. Related Controls:
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordinatio Applicability: All ASSESSMENT PROCEDURE: PL-6.1 Assessment Objective Determine if: (i) the organization plans and coordinates securit organizational assets, and individuals; and	iduals. Routine security-related activities include, but are not limited to, security assessments irganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so on includes both emergency and non-emergency (i.e., routine) situations. References: ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations. ecurity certifications, and testing/exercises. Related Controls:
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordinatic Applicability: All ASSESSMENT PROCEDURE: PL-6.1 Assessment Objective Determine if: (i) the organization plans and coordinates securi organizational assets, and individuals; and (ii) the organization's advance planning and coordinates	iduals. Routine security-related activities include, but are not limited to, security assessments irganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so on includes both emergency and non-emergency (i.e., routine) situations. References: ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations. ecurity certifications, and testing/exercises. Related Controls:
and reputation), organizational assets, and indivise security certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordinatio Applicability: All ASSESSMENT PROCEDURE: PL-6.1 Assessment Objective Determine if: (i) the organization plans and coordinates securi organizational assets, and individuals; and (ii) the organization's advance planning and coor Assessment Methods And Objects	iduals. Routine security-related activities include, but are not limited to, security assessments irganizational advance planning and coordination includes both emergency and non-emergence enot limited to, security assessments, audits, system hardware and software maintenance, so includes both emergency and non-emergency (i.e., routine) situations. References: ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6 ty-related activities affecting the information system before conducting such activities in order rdination of security-related activities includes both emergency situations	s, audits, system hardware and software maintenance, acy (i.e., routine) situations. ecurity certifications, and testing/exercises. Related Controls:
and reputation), organizational assets, and indivise curity certifications, and testing / exercises. O Guidance Routine security-related activities include, but are Organizational advance planning and coordinatic Applicability: All ASSESSMENT PROCEDURE: PL-6.1 Assessment Objective Determine if: (i) the organization plans and coordinates securit organizational assets, and individuals; and (ii) the organization's advance planning and coordinates Assessment Methods And Objects Examine: Security planning policy; procedures a	iduals. Routine security-related activities include, but are not limited to, security assessments irganizational advance planning and coordination includes both emergency and non-emergen e not limited to, security assessments, audits, system hardware and software maintenance, so on includes both emergency and non-emergency (i.e., routine) situations. References: ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6	s, audits, system hardware and software maintenance, ncy (i.e., routine) situations. ecurity certifications, and testing/exercises. Related Controls:

Personnel Security (PS) – Operational

PS-1 – Personnel Security Policy and I	Procedures (High)	
Control		
CMS information systems shall employ person	nel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations,	standards, and guidelines. Procedures shall t
developed to guide the implementation of pers	onnel security controls.	
Guidance		
The personnel security policy and procedures	are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and g	juidance. The personnel security policy can be
	urity policy for the organization. Personnel security procedures can be developed for the security progra	am in general, and for a particular information
	des guidance on security policies and procedures.	
Applicability: All	References: ARS: PS-1; FISCAM: TSD-1.3.3; IRS-1075: 5.6.2.1#1.1-2; NIST 800-53/53A: PS-1; PISP: 4.13.1	Related Controls:
ASSESSMENT PROCEDURE: PS-1.1		- F
Assessment Objective		
Determine if:		
(i) the organization develops and documents p		
	curity policy and procedures to appropriate elements within the organization;	
	periodically review personnel security policy and procedures; and	
	y policy and procedures when organizational review indicates updates are required.	
Assessment Methods And Objects		
Examine: Personnel security policy and proce		
Interview: Organizational personnel with person	onnel security responsibilities.	
ASSESSMENT PROCEDURE: PS-1.2		
Assessment Objective		
Determine if:		
	pose, scope, roles and responsibilities, management commitment, coordination among organizational e	
	vith the organization's mission and functions and with applicable laws, directives, policies, regulations, s	
	all areas identified in the personnel security policy and address achieving policy-compliant implementa	tions of all associated security controls.
		······································
		·····,···
Examine: Personnel security policy and proce		···· , ···
Examine: Personnel security policy and proce Interview: Organizational personnel with person		···· , ··· , ···
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High)		
Examine: Personnel security policy and proce Interview: Organizational personnel with perso PS-1(FIS-1) – Enhancement (High) Control	onnel security responsibilities.	
Examine: Personnel security policy and proce Interview: Organizational personnel with perso PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic	onnel security responsibilities. basis and controlled to ensure that objectives laid out in job descriptions are carried out.	
Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1	
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective Determine if the organization monitors staff pe	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective Determine if the organization monitors staff per Assessment Methods And Objects	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective Determine if the organization monitors staff pe Assessment Methods And Objects Examine: Pertinent policies and procedures.	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1 rformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective Determine if the organization monitors staff pe Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions requiring	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1 rformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are are and supervisory review and approval for evidence of such performance (e.g., approval of input of transaction)	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions requirin Interview: Management and subordinate pers	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1 rformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are are and supervisory review and approval for evidence of such performance (e.g., approval of input of transaction)	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective Determine if the organization monitors staff pe Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions requiring	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1 rformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are are and supervisory review and approval for evidence of such performance (e.g., approval of input of transaction)	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective Determine if the organization monitors staff pe Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions requirin Interview: Management and subordinate person	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1 rformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are are and supervisory review and approval for evidence of such performance (e.g., approval of input of transaction)	Related Controls:
Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (High) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1).1 Assessment Objective Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions requiring Interview: Management and subordinate person PS-1(FIS-2) – Enhancement (High) Control	basis and controlled to ensure that objectives laid out in job descriptions are carried out. References: FISCAM: TSD-2.2.1 rformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are are and supervisory review and approval for evidence of such performance (e.g., approval of input of transaction)	Related Controls:

ASSESSMENT PROCEDURE: PS-1(FIS-2).1

Assessment Objective

Determine if the organization regularly schedules vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.

Assessment Methods And Objects

Examine: Personnel records to identify individuals who have not taken vacation or sick leave in the past year.

Examine: Staff assignment records and determine whether job and shift rotations occur.

Examine: Vacation and job rotation policies and procedures.

Interview: Information system management and users.

PS-1(FIS-3) – Enhancement (High)

Control

Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes. Employees are made aware of their job descriptions.

Applicability: All	References: FISCAM: TSD-1.2.2, TSD-1.3.1, TSP-4.2.1, TSS-2.1.2, TSS-2.1.3	Related Controls:

ASSESSMENT PROCEDURE: PS-1(FIS-3).1

Assessment Objective

Determine if:

(i) the organizational documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes.

(ii) the organization makes the employees aware of their job descriptions.

Assessment Methods And Objects

Examine: Effective dates of the position descriptions and determine whether they are current.

Examine: Job descriptions for several positions in organizational units and for user security administrators.

Examine: Job descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.

Interview: Management personnel.

PS-2 – Position Categorization (High)

Control

A criticality / sensitivity rating (e.g., non-sensitive, national security, public trust) shall be assigned to all positions within the organization. The criticality / sensitivity rating shall be in compliance with 5 CFR 731.106(a), Executive Orders 10450 and 12968, NSPD-1, HSPD-7, and HSPD-12 and consistent with OPM policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating. All criticality / sensitivity ratings must be submitted to the DHHS HR department and CMS' personnel security department.

Guidance

Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Applicability: All	References: ARS: PS-2; IRS-1075: 5.6.2.1#1.3; NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:

ASSESSMENT PROCEDURE: PS-2.1

Assessment Objective

Determine if:

(i) the organization assigns a risk designations to all positions within the organization;

(ii) the organization establishes a screening criteria for individuals filling organizational positions;

(iii) the risk designations for the organizational positions are consistent with applicable federal regulations and OPM policy and guidance;

(iv) the organization defines the frequency of risk designation reviews and updates for organizational positions; and

(v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan; records of risk designation reviews and updates; other relevant documents or records.

PS-2(0) – Enhancement (High)

Control

Review and revise position risk designations every 365 days.

Applicability: All	References: ARS: PS-2(0); NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:
ASSESSMENT PROCEDURE: PS-2(0).1		
Assessment Objective		
Determine if the organization meets the re	quirements as specified in the baseline control and the specific CMS requirements as prescribed in this am	plifying enhancement to the baseline control.
ssessment Methods And Objects		
positions; information system security plar	edures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidan n (for organization-defined frequency for review of position categorizations); records of risk designation revie	
records. PS-3 – Personnel Screening (High)		
	tes and contractors who require access to CMS information or information systems shall be screened and re For prospective employees, references background checks shall be performed before issuance of a User ork with mission critical information.	
Guidance		
	1.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regu a established for the risk designation of the assigned position.	lations, and guidance; (iv) FIPS 201 and SP 80
Applicability: All	References: ARS: PS-3; FISCAM: TSP-4.1.1, TSP-4.1.2; IRS-1075: 5.6.2.1#1.4; NIST 800-53/53A PS-3; PISP: 4.13.3	Related Controls:
ASSESSMENT PROCEDURE: PS-3.1		
risk designation for the assigned position. Assessment Methods And Objects Examine: Personnel security policy; proce records. PS-3(0) – Enhancement (High) Control	edures addressing personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76	6, and 800-78; other relevant documents or
Perform criminal history check for all perso	ons prior to employment.	
Applicability: All	References: ARS: PS-3(0); FISCAM: TSP-4.1.2; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:
ASSESSMENT PROCEDURE: PS-3(0).1		
Assessment Objective Determine if the organization meets the re Assessment Methods And Objects	equirements as specified in the baseline control and the specific CMS requirements as prescribed in this am	
Examine: Personnel security policy; proce	edures for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 80	
Examine: Personnel security policy; proce S-3(CMS-1) – Enhancement (High) control	edures for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 80	
Examine: Personnel security policy; proce S-3(CMS-1) – Enhancement (High) Control Require personnel to obtain and hold a hig	edures for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 80	0-78; other relevant documents or records.
Examine: Personnel security policy; proce PS-3(CMS-1) – Enhancement (High) Control	edures for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 80 gh-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook. References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	
Examine: Personnel security policy; proce S-3(CMS-1) – Enhancement (High) Control Require personnel to obtain and hold a high pplicability: All SSESSMENT PROCEDURE: PS-3(CMS Assessment Objective Determine if: (i) the organization screens individuals recommended (i) the organization screens individuals recommended (ii) the organization screens individuals recommended (iii) the organization screens individuals	edures for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 80 gh-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook. References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	0-78; other relevant documents or records. Related Controls:

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; and other relevant documents or records to determine that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

Interview: Personnel with personnel screening responsibilities to confirm that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

PS-4 – Personnel Termination (High)

Control

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information and information systems is removed upon personnel termination. Termination procedures shall address:

4.13.4.1. Exit interviews;

4.13.4.2. Retrieval of all organizational information system-related property;

4.13.4.3. Notification to security management;

4.13.4.4. Revocation of all system access privileges;

4.13.4.5. Immediately escorting employees terminated for cause out of organization facilities; and

4.13.4.6. Hard disk back up and sanitization before re-issuance.

Appropriate personnel shall have access to official records created by the terminated employee that are stored on organizational information systems.

Guidance

Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Applicability: All	References: ARS: PS-4; FISCAM: TAC-2.1.6, TSP-4.1.6; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075:	Related Controls:
	5.6.2.1#1.5; NIST 800-53/53A: PS-4; PISP: 4.13.4	

ASSESSMENT PROCEDURE: PS-4.1

Assessment Objective

Determine if:

(i) the organization terminates information system access upon termination of individual employment;

(ii) the organization conducts exit interviews of terminated personnel;

(iii) the organization retrieves all organizational information system-related property from terminated personnel; and

(iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.

PS-4(CMS-1) – Enhancement (High) Control Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

during the employee termination process.			
Applicability: All	References: ARS: PS-4(CMS-1); FISCAM: TAC-3.2.C.4	Related Controls:	
ASSESSMENT PROCEDURE: PS-4(CMS-1).1			

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process. **Interview:** Personnel with termination responsibilities to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

PS-5 – Personnel Transfer (High)

Control

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information or information systems no longer required in the new assignment is

terminated upon personnel transfer. Transfer procedures shall address:

4.13.5.1. Re-issuing appropriate organizational information system-related property (e.g., keys, identification cards, building passes);

4.13.5.2. Notification to security management;

4.13.5.3. Closing obsolete accounts and establishing new accounts: and

4.13.5.4. Revocation of all system access privileges (if applicable).

Guidance

Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing

system access autionizations, and (iv) providing for access to onicial records created or controlled by the employee at the old work location and in the old accounts.			
Applicability: All	References: ARS: PS-5; FISCAM: TAC-2.1.6, TSP-4.1.6; IRS-1075: 5.6.2.1#1.6; NIST 800-53/53A:	Related Controls:	
	PS-5; PISP: 4.13.5		
ASSESSMENT PROCEDURE: PS-5.1			

Assessment Objective

Determine if:

(i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and

(ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

PS-6 – Access Agreements (High)

Control

Individuals who require access to CMS information or information systems shall be required to complete and sign appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements.

Guidance

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Applicability: All	References: ARS: PS-6; FISCAM: TSP-4.1.3; IRS-1075: 5.6.2.1#1.7; NIST 800-53/53A: PS-6; PISP: 4.13.6	Related Controls:
	15.0	

ASSESSMENT PROCEDURE: PS-6.1

Assessment Objective

Determine if:

(i) the organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access;

(ii) organizational personnel sign access agreements;

(iii) the organization defines the frequency of reviews and updates for access agreements; and

(iv) the organization reviews and updates the access agreements in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan; access agreements; records of access agreement reviews and updates: other relevant documents or records.

r 3-6(0) – Elimancement (riigit)			
Control			
Access agreements are reviewed and updated as part of the system accreditation or when a contract is renewed or extended.			
Applicability: All	References: ARS: PS-6(0); NIST 800-53/53A: PS-6; PISP: 4.13.6	Related Controls:	
ASSESSMENT PROCEDURE: PS-6(0).1			
Assessment Objective			
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.			
Assessment Methods And Objects			

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan (for organization-defined Page 145 of 207 Rev. 9

frequency for access agreement reviews); acces	ss agreements; records of access agreement reviews and updates; other rele	vant documents or records.	
PS-7 – Third-Party Personnel Security (
Control	(
Personnel security controls employed by externa provisions for security clearances, background of	al service providers and third parties shall be documented, agreed to, implem checks, required expertise, defined security roles and responsibilities, and con th CMS IS policies and procedures, and consistent with NIST SP 800-35.		
	ce bureaus, contractors, and other organizations providing information syster anization explicitly includes personnel security requirements in acquisition-re		
Applicability: All	References: ARS: PS-7; IRS-1075: 5.6.2.1#1.8; NIST 800-53/53A: PS-7; F	ISP: 4.13.7 Rela	ated Controls:
ASSESSMENT PROCEDURE: PS-7.1			
Assessment Objective			
providing information system development, infor (ii) the organization explicitly includes personnel (iii) the organization monitors third-party provide Assessment Methods And Objects	ty requirements, including security roles and responsibilities, for third-party pr mation technology services, outsourced applications, network and security m security requirements in acquisition-related documents in accordance with N r compliance with personnel security requirements.	anagement); IST SP 800-35; and	
	nnel security responsibilities; third-party providers.		
PS-7(CMS-1) – Enhancement (High)			
Control			
Regulate the access provided to contractors and	d define security requirements for contractors. Contractors must be provided e contractor selection process must assess the contractor's ability to adhere t		
Applicability: All	References: ARS: PS-7(CMS-1)		ated Controls:
ASSESSMENT PROCEDURE: PS-7(CMS-1).1			
providing information system development, infor (ii) the organization monitors third-party provider Assessment Methods And Objects	ty requirements, including security roles and responsibilities, for third-party pr mation technology services, outsourced applications, network and security m r compliance with personnel security requirements.	anagement); and	
relevant documents or records to determine the	access provided to contractors and defining security requirements for contra S information security requirements. The contractor selection process must a	tors. Contractors must be provid	ed with minimal system and physical
	and a self-1992 and the distance been directed as a second second distance to the strength of the second se	within the ecourity requirements	
to adhere to and support CMS' information secu	sponsibilities to determine that the access provided to contractors are defined ss, and must agree to and support the CMS information security requirement rity policies, and standards.		
to adhere to and support CMS' information secu	ss, and must agree to and support the CMS information security requirement		
to adhere to and support CMS' information secu PS-8 – Personnel Sanctions (High) Control	ess, and must agree to and support the CMS information security requirement rity policies, and standards.	s. The contractor selection proce	ss must assess the contractor's ability
to adhere to and support CMS' information secu PS-8 – Personnel Sanctions (High) Control The organization shall enforce formal personnel	ss, and must agree to and support the CMS information security requirement	s. The contractor selection proce	ss must assess the contractor's ability
to adhere to and support CMS' information secu PS-8 – Personnel Sanctions (High) Control The organization shall enforce formal personnel consistent with applicable laws, Executive Order Guidance	ss, and must agree to and support the CMS information security requirement rity policies, and standards. sanctions process for personnel who fail to comply with established CMS IS rs, policies, directives, regulations, standards, and guidelines.	s. The contractor selection proce	ss must assess the contractor's ability ployee sanction process shall be
to adhere to and support CMS' information secu PS-8 – Personnel Sanctions (High) Control The organization shall enforce formal personnel consistent with applicable laws, Executive Order Guidance	ss, and must agree to and support the CMS information security requirement rity policies, and standards. sanctions process for personnel who fail to comply with established CMS IS rs, policies, directives, regulations, standards, and guidelines.	s. The contractor selection proce	ss must assess the contractor's ability ployee sanction process shall be

Applicability: All	References: ARS: PS-8; HIPAA: 164.308(a)(1)(ii)(C); NIST 800-53/53A: PS-8; PISP: 4.13.8	Related Controls:
ASSESSMENT PROCEDURE: PS		
Assessment Objective		
Determine if:		
	al sanctions process for personnel failing to comply with established information security policies and procedures	; and
	s is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
Assessment Methods And Objec		
	y; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant docu	iments or records.
PS-CMS-1 – Review System A	ccess during Extraordinary Personnel Circumstances (High)	
Control		
Access to CMS information and inf	ormation systems shall be reviewed during extraordinary personnel circumstances and limited as deemed neces	sary.
Guidance		
	onal problems could be considered extraordinary personal circumstances. For some personnel, recovery from a c cumstances on a case by case basis.	difficult time may take longer than usual and
Applicability: All	References: ARS: PS-9; PISP: 4.13.9	Related Controls:
ASSESSMENT PROCEDURE: PS		Related Controls.
Assessment Objective		
	ages personnel with extraordinary personal circumstances.	
Assessment Methods And Objec		
		simulation is an investigated and some in limited
as deemed necessary.	y and procedures; other relevant documents or records determine system access during extraordinary personnel	circumstances is reviewed and access is limited
,	el with personnel security responsibilities to determine system access during extraordinary personnel circumstan	ces is reviewed and access is limited as deemed
necessary.	- · · · · · · · · · · · · · · · · · · ·	
PS-CMS-2 – Designate an Info	rmation System Security Officer (ISSO) / System Security Officer (SSO) (High)	
Control		
An Information System Security Of	ficer (ISSO) / System Security Officer (SSO) shall be designated for each business component with roles and res	ponsibilities of the position clearly defined.
Guidance		· · · ·
	ne Information System Security Officer (ISSO) / System Security Officer (SSO) responsibilities are the NIST SPs.	Specific responsibilities should be developed to
protect CMS information systems a		
	References: ARS: PS-10; FISCAM: TSP-3.1.1, TSP-3.1.2; HIPAA: 164.308(a)(2); PISP: 4.13.10	Related Controls:
ASSESSMENT PROCEDURE: PS	-CMS-2.1	
Assessment Objective		
•	locumented the roles and responsibilities of appointed ISSO / SSO.	
Assessment Methods And Objec		
Examine: Personnel security polic clearly defined.	y and procedures; other relevant documents or records to determine an ISSO / SSO is designated for each comp	onent with roles and responsibilities of the position
Interview: Organizational personn defined.	el with personnel security responsibilities to determine an ISSO / SSO is designated for each component with role	es and responsibilities of the position clearly

Risk Assessment (RA) - Management

RA-1 – Risk Assessment Policy and Procedures (High)

Control

All CMS applications and systems shall be covered by an IS RA. The RA shall be consistent with NIST SP 800-30. Formal documented procedures shall be developed, disseminated, and reviewed / updated periodically to facilitate the implementation of the RA policy and associated RA controls. The procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-30 provides guidance on the assessment of risk. NIST SP 800-12 provides guidance on security policies and procedures.

	- gamman	
Applicability: All	References: ARS: RA-1; FISCAM: TAC-3.1.A.2; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075:	Related Controls:
	5.6.1.1#1.1-2; NIST 800-53/53A: RA-1; PISP: 4.14.1	

ASSESSMENT PROCEDURE: RA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents risk assessment policy and procedures;

(ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization;

- (iii) responsible parties within the organization periodically review risk assessment policy and procedures; and
- (iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

ASSESSMENT PROCEDURE: RA-1.2

Assessment Objective

Determine if:

(i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

RA-2 – Security Categorization (High)

Control

CMS information systems and the information processed, stored, or transmitted by the systems shall be categorized in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to the, CMS System Security Level by Information Type. The security categorization (including supporting rationale) shall be explicitly documented. Designated senior-level officials within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the CMS CIO, CISO, and Business Owners.

All CMS information systems categorized as high or moderate shall be considered sensitive or to contain sensitive information. All CMS information systems categorized as low shall be considered non-sensitive or to contain non-sensitive information. All CMS information systems shall implement minimum security requirements and controls as established in the current CMS IS Standards, based on security categorization of the system.

Guidance

The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST SP 800-60 provides guidance on determining the security categories of the

information types resident on the information system Applicability: All References: ARS: RA-2; FISCAM: TAC-1.1; HSPD 7: D(8); IRS-1075; 4.1#2; NIST 800-53/53A: RA-Related Controls: MP-4, SC-7 2: PISP: 4.14.2 **ASSESSMENT PROCEDURE: RA-2.1 Assessment Objective** Determine if: (i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners; (ii) the security categorization is consistent with FIPS 199 and NIST SP 800-60; (iii) the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts: (iv) the organization includes supporting rationale for impact-level decisions as part of the security categorization; and (v) designated, senior-level organizational officials review and approve the security categorization of the information system. Assessment Methods And Objects Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST SP 800-60; information system security plan; other relevant documents or records. Interview: Organizational personnel with security categorization and risk assessment responsibilities. RA-3 – Risk Assessment (RA) (High) Control An assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information systems that support the operations and assets of CMS shall be performed, both within CMS and by external parties that manage / operate information or information systems for CMS. The RA shall be in accordance with current CMS Procedures. Based on the operation of the information system, the RA shall take into account vulnerabilities, threat sources, and security controls in place to determine the resulting level of residual risk posed to CMS operations. CMS assets. CMS information, or individuals. Any findings from reviews of CMS systems shall be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses shall be documented by the Business Owner or external party and addressed by mitigating the risk, accepting the risk with explanation or submitting Corrective Action Plan (CAP). These findings shall be subject to reporting requirements as established by applicable laws. Executive Orders, directives, policies, regulations, standards, and guidance. Guidance Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST SP 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments. Applicability: All References: ARS: RA-3; FISCAM: TAC-3.1.A.2, TSP-1.1.2, TSP-1.1.3, TSP-5.1.4; HIPAA: **Related Controls:** 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3. 6.3.3#2: NIST 800-53/53A: RA-3: PISP: 4.14.3 **ASSESSMENT PROCEDURE: RA-3.1 Assessment Objective** Determine if: (i) the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and (ii) the risk assessment is consistent with the NIST SP 800-30. **Assessment Methods And Objects**

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST SP 800-30; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

RA-32(NIS-1) - Enhancement (High) Control Perform an IS RA for the system, and document the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]). Applicability: All References: ARS: RA-3(CMS-1); FISCAM: TAC-1.1, TAC-1.2, TSS-2.2.4; HIPAA: 164.306(a)(2); Related Controls: ASSESSMENT PROCEDURE: RA-3(CMS-1).1 Assessment Objective Reservence: Assessment objective in the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties). Assessment Objective Reservence: Rethose Add Objects Reservence: Rethose Add Objects Reservence: Rethose Add Objects Examine: Rick assessment policy: security planing policy and procedures: procedures addressing organization adormetion that protor project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]). Interview: Organization alpersonnel with risk assessment update: Assessment to project initiation, the organization performs an IS RA for the system, and documents responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents responsibilities to determine that prior to project initiation, the organization develops and documented every three (3) years or whenever			
Perform an IS RA for the system, and document the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK). Applicability: All References: ARS: RA-3(CMS-1); FISCAM: TAC-1.1, TAC-1.2, TSS-2.2.4; HIPAA: 164.306(a)(2); Related Controls: ASSESSMENT PROCEDURE: RA-3(CMS-1).1 Assessment Objective Determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties). Assessment Objective Assessment Methods And Objects Examine: Risk assessment policy, security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment, information system security plan (for organization defined frequency for risk assessment updates; NIST SP 800-30; other relevant documents to records to determine that prior to project initiation, the organization aperforms an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK)). Interview: Organizational personnel with risk assessment updates; NIST SP 800-30; other relevant documents or records to determine that prior to project initiation, the organization performs an IS RA for the system, and documents excurity Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK)). Interview: Organization develops and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in securit, a sustasset, Accredit	RA-3(CMS-1) – Enhancement (High)		
Investment Framework [FRAMEWORK]). References: ARS: RA:3(CMS-1); FISCAM: TAC-1.1, TAC-1.2, TSS-2.2.4; HIPAA: 164.306(a)(2); Related Controls: Assessment Objective Assessment Objective Assessment Objection Assessment Comparization and assets (including information and information systems managed/operated by external parties). Assessment Methods And Objects Examine: Risk assessment policy: security planning policy and procedures: procedures addressing organization and assess (including information ad assess (including information ad information systems managed/operated by external parties). Assessment (FRAMEWORK). Assessment Wethods And Objects Examine: Risk assessment policy: security planning policy and procedures is procedures addressing organization addressing organization addressing organization performs an IS RA for the system. Termework (FRAMEWORK). RA Interview: Organization performs an IS RA for the system. In accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK). RA RA-4 - RISK Assessment Update: (High) Control Control References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: Related Contr	Control		
HSPD 7: D(8), F(19) ASSESSMENT PROCEDURE: RA-3(CMS-1).1 Assessment Objective Determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information and information systems that support its operations and assets (including information and information systems managed/operated by external parties). Assessment Methods And Objects Examine: Risk assessment policy: security planning policy and procedures; procedures addressing organizational assessment documents or records to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK)). Interview: Organization performs and ISRA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK)). RA-4 - Risk Assessment Update (High) Control The A shall be performed and documented every three (3) years or whenever there are significant changes to the system. facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation. Guidance References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: Related Controls:		t the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessme	nt (RA) Procedures (See CMS Integrated IT
Assessment Objective Determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties). Assessment Methods And Objects Examine: Risk assessment policy: security planning policy and procedures: procedures addressing organizational assessments of risk; risk assessment policy: security planning policy and procedures: procedures addressing organizational assessments or records to determine that prior to project initiation, the organization-defined frequency for risk assessment (RAN Procedures); NIST SP 800-30; other relevant documents or records to determine that prior to project initiation, the organization all personnel with risk assessment (RAN Procedures); See CMS Integrated IT Investment Framework [FRAMEWORK]). Interview: Organizational personnel with risk assessment responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]). RA-4 – Risk Assessment Update (High) Control The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system. facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation. Guidance The organization develops and documents specific criteria for what is considered significant changes to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates; (1), G(24); IRS-1075: 5.6.1.1#14; NIST 800-53/53A; RA-4; PISP: 4.1.4, ASSESSMENT PROCEDURE; RA-4.1 Assessment Objec	Applicability: All		Related Controls:
Determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information systems managed/operated by external parties). Assessment Methods And Objects Examine: Risk assessment updates; iscoreds of risk assessment updates; iscored risk assessment risks and asfeguards of the system; and accuments responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and asfeguards of the system; facilities, or other conditions that may impact the security or accreditation astatus of the system. Further, the requirements for re-assessments are listed in section	ASSESSMENT PROCEDURE: RA-3(CMS-1).		·
information systems that support its operations and assets (including information and information systems managed/operated by external parties). Assessment Methods And Objects Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; information system security plan (for organization-defined frequency for risk assessment updates); records of risk assessment updates; NIST SP 800-30; other relevant documents or records to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]). Interview: Organization performed with risk assessment responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]). RA4 - RISK Assessment Update (High) Control The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation. Guidance The organization develops and documents specific criteria for what is considered significant changes to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates.	Assessment Objective		
Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organization of risk; risk assessment; information system security plan (for organization-defined frequency for risk assessment updates; Irecords of risk assessment updates; IST SP 800-30; other relevant documents or records to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK)). Interview: Organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK)). RA4 - Risk Assessment Update (High) Control The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation. Guidance References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.1.4.4 Related Controls: Assessment Objective Determine if: (i) the organization defines the risk assessment updates; (ii) the organization system, the facilities where the system; exide, or other conditions that may impact the security or accreditation status of the system; (ii) the organization develops and docume	information systems that support its operations		ication, or destruction of information and
organization-defined frequency for risk assessment updates); records of risk assessment updates; NIST SP 800-30; other relevant documents or records to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]). Interview: Organizational personnel with risk assessment responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework [FRAMEWORK]). RA-4 - Risk Assessment Update (High) Control The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6. Security Accreditation. Guidance The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates. Applicability: All References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: Related Controls: Assessment Objective Determine if: (i) the organization updates the risk assessment updates; (ii) the organization updates the risk assessment updates; (ii) the organization	-		the formula of the second s
Interview: Organizational personnel with risk assessment responsibilities to determine that prior to project initiation, the organization performs an IS RA for the system, and documents the risks and safeguards of the system in accordance with the CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (FRAMEWORK)). RA-4 – Risk Assessment Update (High) Control The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation. Guidance The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates. Applicability: All References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(10), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(10), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(10), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(10), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(10), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(10), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(10), G(24); IRS-1075; 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164	organization-defined frequency for risk assessm the organization performs an IS RA for the syste	ent updates); records of risk assessment updates; NIST SP 800-30; other relevant documents or records em, and documents the risks and safeguards of the system in accordance with the CMS Information Sect	s to determine that prior to project initiation,
RA-4 – Risk Assessment Update (High) Control The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation. Guidance The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates. Applicability: All References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: [19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCP: 4.14.4 Assessment Objective Determine if: (i) the organization defines the frequency of risk assessment updates; (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects	Interview: Organizational personnel with risk as safeguards of the system in accordance with the	esessment responsibilities to determine that prior to project initiation, the organization performs an IS RA CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Fram	for the system, and documents the risks and nework [FRAMEWORK]).
The RA shall be performed and documented every three (3) years or whenever there are significant changes to the system, facilities, or other conditions that may impact the security or accreditation status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation. Guidance The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates. Applicability: All References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4 Related Controls: Assessment Objective Determine if: iiii the organization updates the risk assessment updates; iiii the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the organization update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects And Objects	RA-4 – Risk Assessment Update (High)		
status of the system. Further, the requirements for re-assessments are listed in section 4.4.6, Security Accreditation. Guidance The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates. Applicability: All References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; FISCP.4.1.4 Assessment Objective Determine if: (i) the organization defines the frequency of risk assessment updates; (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects	Control		
The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates. Applicability: All References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4 Related Controls: ASSESSMENT PROCEDURE: RA-4.1 Assessment Objective Determine if: (i) the organization defines the frequency of risk assessment updates; (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects			that may impact the security or accreditation
updates. References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: Related Controls: Assessment Objective F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4 Related Controls: Determine if: (i) the organization defines the frequency of risk assessment updates; iii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects Assessment Methods And Objects	Guidance		
F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4 ASSESSMENT PROCEDURE: RA-4.1 Assessment Objective Determine if: (i) the organization defines the frequency of risk assessment updates; (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects		ific criteria for what is considered significant change to the information system. NIST SP 800-30 provides	s guidance on conducting risk assessment
Assessment Objective Determine if: (i) the organization defines the frequency of risk assessment updates; (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects	Applicability: All		Related Controls:
Determine if: (i) the organization defines the frequency of risk assessment updates; (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects	ASSESSMENT PROCEDURE: RA-4.1		
 (i) the organization defines the frequency of risk assessment updates; (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. 	Assessment Objective		
 (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects			
system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects	., .	•	the former of the second second by the first With second second by
 (iii) the risk assessment update is consistent with the NIST SP 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects 			e information system, the facilities where the
(iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation. Assessment Methods And Objects			
	Assessment Methods And Objects		
Examine: Risk assessment policy; security planning policy and procedures; procedures addressing risk assessment updates; risk assessment; information system security plan; records of risk			ion system security plan; records of risk
assessment updates; NIST SP 800-30; other relevant documents or records.		evant documents or records.	
RA-5 – Vulnerability Scanning (High)	RA-5 – Vulnerability Scanning (High)		
Control			
Appropriate vulnerability assessment tools and techniques shall be implemented by the organization. Selected personnel shall be trained in their use and maintenance. The organization shall conduct periodic testing of its security posture by scanning its information systems with vulnerability tools. The information obtained from the vulnerability scanning process shall be shared with	conduct periodic testing of its security posture b	y scanning its information systems with vulnerability tools. The information obtained from the vulnerabilit	y scanning process shall be shared with
appropriate personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems. The activities of employees using organization Internet and email resources shall be subject to monitoring by system or security personnel without notice.			ctivities of employees using organization
Guidance			
Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST SP 800-42 provides guidance on	techniques. Vulnerability scans are scheduled a freely shared with appropriate personnel through	nd/or random in accordance with organizational policy and assessment of risk. The information obtained nout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability a	from the vulnerability scanning process is nalysis for custom software and applications
Rev. 9 Page 150 of 207 BPSSM Appendix A, Attachment 1	· · · · · · · · · · · · · · · · · · ·		, , , , , , , , , , , , , , , , , , , ,

network security testing. NIST SP 800-40 (Versi	on 2) provides guidance on patch and vulnerability management.			
Applicability: All	References: ARS: RA-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5; PISP: 4.14.5	Related Controls:		
ASSESSMENT PROCEDURE: RA-5.1				
Assessment Objective				
Determine if:				
(i) the organization defines the frequency of vuln				
and reported;	e information system in accordance with the organization-defined frequency or when significant new vulr			
vulnerability management process by using stan	ools and techniques to conduct the vulnerability scans including those tools that ensure interoperability a dards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and make the test of the sector of			
procedures, and (c) measuring vulnerability impa	ity scanning in accordance with NIST SP 800-42; and			
	lity management in accordance with NIST SP 800-42, and			
Assessment Methods And Objects				
Examine: Risk assessment policy; procedures a management records; other relevant documents	uddressing vulnerability scanning; risk assessment; information system security plan; vulnerability scanni	ng results; patch and vulnerability		
	sessment and vulnerability scanning responsibilities.			
RA-5(0) – Enhancement (High)				
Control	nd techniques to scan for vulnerabilities in the information system every 90 days or when significant new	vulnorabilities are identified and reported		
Applicability: All	References: ARS: RA-5(0); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5;	Related Controls:		
	PISP: 4.14.5	Related Controls.		
ASSESSMENT PROCEDURE: RA-5(0).1				
Assessment Objective				
Determine if the organization meets the requiren	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ing enhancement to the baseline control.		
Assessment Methods And Objects				
	ddressing vulnerability scanning; risk assessment; information system security plan (for organization-del	ined frequency for vulnerability scanning);		
	bility management records; other relevant documents or records.			
	sessment and vulnerability scanning responsibilities.			
RA-5(1) – Enhancement (High)				
Control				
	ability to readily update the list of vulnerabilities scanned.			
Applicability: All	References: ARS: RA-5(1); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5(1)	Related Controls:		
ASSESSMENT PROCEDURE: RA-5(1).1				
Assessment Objective				
Determine if:				
	bols that have the capability to readily update the list of information system vulnerabilities scanned; and			
(ii) the vulnerability scanning tools retrieve updated lists of information system vulnerabilities from the National Vulnerability Database (NVD).				
	Assessment Methods And Objects			
and vulnerability management records; other rele	ddressing vulnerability scanning; risk assessment; vulnerability scanning tools and techniques documen	tation; vulnerability scanning results; patch		
Test: Vulnerability scanning capability and asso				
RA-5(2) – Enhancement (High)				
Control				
	every 365 days or when significant new vulnerabilities are identified and reported.			
Applicability: All	References: ARS: RA-5(2); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5(2)	Related Controls:		

ASSESSMENT PROCEDURE: RA-5(2).1 Assessment Objective Determine if: (i) the organization defines the frequency of updates for information system vulnerabilities scanned: and (ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when significant new vulnerabilities are identified and reported. Assessment Methods And Objects Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records. RA-5(3) – Enhancement (High) Control Perform internal network penetration testing as needed but no less than once a year, in accordance with the CMS IS procedures. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention. References: ARS: RA-5(3); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5(3) Applicability: All Related Controls: **ASSESSMENT PROCEDURE: RA-5(3).1** Assessment Objective Determine if: (i) the organization implements procedures that can demonstrate the breadth of scan coverage (including information system components scanned); and (ii) the organization implements procedures that can demonstrate the depth of scan coverage (including vulnerabilities checked). **Assessment Methods And Objects** Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and information system components checked; other relevant documents or records.(Optional) RA-5(CMS-1) – Enhancement (High) Control Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once a year, in accordance with CMS IS procedures. Document findings and assessment results and correlate vulnerabilities to Common Vulnerabilities and Exposures (CVE) naming convention. Applicability: All References: ARS: RA-5(CMS-1); HIPAA; 164,306(a)(2); HSPD 7; F(19), G(24) **Related Controls:** ASSESSMENT PROCEDURE: RA-5(CMS-1).1 **Assessment Objective** Determine if: (i) the organization defines the frequency of vulnerability scans within the information system; (ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported; and (iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact. Assessment Methods And Objects Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for vulnerability scanning); vulnerability scanning results: patch and vulnerability management records: other relevant documents or records to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE) naming convention. Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE) naming convention.

System and Services Acquisition (SA) – Management

· · ·		
SA-1 – System and Services Acquisition	Policy and Procedures (High)	
Control		
	implemented effectively to facilitate the implementation of the system and services acquisition securi	ty controls in all system and services
acquisitions. Procedures shall be consistent with	applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
Guidance		
The system and services acquisition policy and p	rocedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, star	ndards, and guidance. The system and services
	peneral information security policy for the organization. System and services acquisition procedures c	
	when required. NIST SP 800-12 provides guidance on security policies and procedures.	
Applicability: All	References: ARS: SA-1; IRS-1075: 5.6.1.3#1.1-2; NIST 800-53/53A: SA-1; PISP: 4.15.1	Related Controls:
ASSESSMENT PROCEDURE: SA-1.1		
Assessment Objective		
Determine if:		
	tem and services acquisition policy and procedures;	
	vices acquisition policy and procedures to appropriate elements within the organization;	
	riodically review system and services acquisition policy and procedures; and	
	s acquisition policy and procedures when organizational review indicates updates are required.	
Assessment Methods And Objects		
	v and procedures; other relevant documents or records.	
Interview: Organizational personnel with system	and services acquisition responsibilities.	
ASSESSMENT PROCEDURE: SA-1.2		
Assessment Objective		
Determine if:		
	resses purpose, scope, roles and responsibilities, management commitment, coordination among org	
	consistent with the organization's mission and functions and with applicable laws, directives, policies,	
 (iii) the system and services acquisition procedur security controls. 	es address all areas identified in the system and services acquisition policy and address achieving po	licy-compliant implementations of all associated
Assessment Methods And Objects		
Examine: System and services acquisition policy	v and procedures; other relevant documents or records.	
Interview: Organizational personnel with system	and services acquisition responsibilities.	
SA-1(IRS-1) – Enhancement (High)		
Control		
	reviews/updates: (i) a formal, documented, system and services acquisition policy that includes IRS d	locuments received and identified by:
(a) taxpayer name		·····,
(b) tax year(s)		
(c) type of information (e.g., revenue agent repor	ts, Form 1040, work papers)	
(d) the reason for the request		
(e) date requested (f) date received		
(g) exact location of the FTI		
(h) who has had access to the data and		
(i) if disposed of, the date and method of disposit	ion.	
Applicability: All; Optional for ABMAC, CWF, DC,	References: IRS-1075: 3.3#1	Related Controls:
DMEMAC, EDC, PSC, PartA, PartB, SS		
ASSESSMENT PROCEDURE: SA-1(IRS-1).1		
Assessment Objective		
	ates, and periodically reviews/updates; (i) a formal, documented, system and services acquisition pol	icy that includes IPS decuments received and

Determine if the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes IRS documents received and

identified by:

(a) taxpayer name

(b) tax year(s)

(c) type of information (e.g., revenue agent reports, Form 1040, work papers)

(d) the reason for the request

(e) date requested

(f) date received

(g) exact location of the FTI

(h) who has had access to the data and

(i) if disposed of, the date and method of disposition.

Assessment Methods And Objects

Examine: Organizational documentation that contains the development, dissemination and review/updates to FTI IRS documents received that show:

(a) taxpayer name

(b) tax year(s)

(c) type of information (e.g., revenue agent reports, Form 1040, work papers)

(d) the reason for the request

(e) date requested

(f) date received

(g) exact location of the FTI

(h) who has had access to the data and

(i) if disposed of, the date and method of disposition.

SA-2 – Allocation of Resources (High)

Control

As part of the capital planning and investment control processes, CMS or the external organization shall determine, document, and allocate the resources required to protect CMS information systems adequately. IS requirements shall be included in mission / business case planning, and a separate line item shall be established in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Guidance

The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST SP 800-65 provides guidance on integrating security into the capital planning and investment control process.

Applicability: All		References: ARS: SA-2; NIST 800-53/53A: SA-2; PISP: 4.15.2	• •	Related Controls:	

ASSESSMENT PROCEDURE: SA-2.1 Assessment Objective

Determine if:

(i) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system;

(ii) the organization determines security requirements for the information system in mission/business case planning;

(iii) the organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation; and

(iv) the organization's programming and budgeting process is consistent with NIST SP 800-65.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST SP 800-65; other relevant documents or records. **Interview:** Organizational personnel with capital planning and investment responsibilities.

SA-3 – Life Cycle Support (High)

Control

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

Guidance

NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Applicability: All	References: ARS: SA-3; FISCAM: TAY-1.2.1, TCC-1.1.2; NIST 800-53/53A: SA-3; PISP: 4.15.3	Related Controls:

ASSESSMENT PROCEDURE: SA-3.1

Assessment Objective

Determine if:

(ii) the organization uses a sve	he information system using a system development life cycle methodology that includes	information security considerations; and
	stem development life cycle that is consistent with NIST SP 800-64.	
Assessment Methods And Ok	•	
	es acquisition policy; procedures addressing the integration of information security into the entation; other relevant documents or records.	e system development life cycle process; NIST SP 800-64; information system
	sonnel with information security and system life cycle development responsibilities.	
SA-3(CMS-1) – Enhancement		
Control	(
	ion security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CM	IS FRAMEWORK.
Applicability: All	References: ARS: SA-3(CMS-1); FISCAM: TCC-1.1.1	Related Controls:
ASSESSMENT PROCEDURE:	SA-3(CMS-1).1	
Assessment Objective		
Determine if:		
	he information system using a system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes in the system development life cycle methodology that includes includes in the system development life cycle methodology that includes includes in the system development life cycle methodology that includes include	information security considerations; and
Assessment Methods And Ok	stem development life cycle that is consistent with NIST SP 800-64.	
	Djects as acquisition policy; procedures addressing the integration of information security into the security into the integration of information security into the integration security into the integrating security integration s	e system development life system
development life cvcle docum	entation; other relevant documents or records to determine the organization complies wit	h the information security steps of IEEE 12207.0 standard for SDLC. as defined
by CMS and/or the CMS FRAI		
	sonnel with information security and system life cycle development responsibilities to dete	ermine the organization complies with the information security steps of IEEE
	s defined by CMS and/or the CMS FRAMEWORK.	
SA-3(FIS-1) – Enhancement (I	High)	
Control		
Applicability: All	s are prepared by the programmer and reviewed by a programming supervisor. References: FISCAM: TCC-2.1.2	Related Controls:
ASSESSMENT PROCEDURE:		Related Collitiols.
Assessment Objective	SA-5(115-1).1	
•	al detailed system specifications are prepared by the programmer and reviewed by a prog	
Assessment Methods And Ol	DIECTS	
Assessment Methods And Ok Examine: Design system spec	-	
	cifications.	
Examine: Design system spece Examine: Pertinent policies an Interview: Programmer and p	cifications. nd procedures. rogramming supervisor.	
Examine: Design system spece Examine: Pertinent policies and the second	cifications. nd procedures. rogramming supervisor.	
Examine: Design system spece Examine: Pertinent policies an Interview: Programmer and p	cifications. nd procedures. rogramming supervisor.	
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s	cifications. nd procedures. rogramming supervisor.) security specifications shall be included, either explicitly or by reference, in all informatior	n system acquisition contracts based on an assessment of risk in accordance
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s	cifications. nd procedures. rogramming supervisor.	n system acquisition contracts based on an assessment of risk in accordance
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive	cifications. nd procedures. rogramming supervisor.) security specifications shall be included, either explicitly or by reference, in all informatior	n system acquisition contracts based on an assessment of risk in accordance
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive Solicitation Documents	cifications. nd procedures. rogramming supervisor.) security specifications shall be included, either explicitly or by reference, in all informatior	
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive Solicitation Documents Solicitation documents (e.g., R 4.15.4.1. Security capabilities;	cifications. nd procedures. programming supervisor.) security specifications shall be included, either explicitly or by reference, in all information e Orders, directives, policies, regulations, and standards. Request for Proposal) for any CMS information system shall include, either explicitly or by	
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive Solicitation Documents Solicitation documents (e.g., R 4.15.4.1. Security capabilities; 4.15.4.2. Design and developr	cifications. nd procedures. programming supervisor.) security specifications shall be included, either explicitly or by reference, in all information e Orders, directives, policies, regulations, and standards. Request for Proposal) for any CMS information system shall include, either explicitly or by iment processes;	
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive Solicitation Documents Solicitation documents (e.g., R 4.15.4.1. Security capabilities; 4.15.4.2. Design and developr 4.15.4.3. Test and evaluation	cifications. nd procedures. programming supervisor.) security specifications shall be included, either explicitly or by reference, in all information e Orders, directives, policies, regulations, and standards. Request for Proposal) for any CMS information system shall include, either explicitly or by iment processes;	
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive Solicitation Documents Solicitation documents (e.g., R 4.15.4.1. Security capabilities; 4.15.4.2. Design and developr	cifications. nd procedures. programming supervisor.) security specifications shall be included, either explicitly or by reference, in all information e Orders, directives, policies, regulations, and standards. Request for Proposal) for any CMS information system shall include, either explicitly or by iment processes;	
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive Solicitation Documents Solicitation documents (e.g., R 4.15.4.1. Security capabilities; 4.15.4.2. Design and developr 4.15.4.3. Test and evaluation p 4.15.4.4. Documentation.	cifications. nd procedures. programming supervisor.) security specifications shall be included, either explicitly or by reference, in all information e Orders, directives, policies, regulations, and standards. Request for Proposal) for any CMS information system shall include, either explicitly or by iment processes;	reference, security requirements that describe the required:
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive Solicitation Documents Solicitation documents (e.g., F 4.15.4.1. Security capabilities; 4.15.4.2. Design and developr 4.15.4.3. Test and evaluation p 4.15.4.4. Documentation. The requirements in the solicit	cifications. nd procedures. programming supervisor.) security specifications shall be included, either explicitly or by reference, in all information e Orders, directives, policies, regulations, and standards. Request for Proposal) for any CMS information system shall include, either explicitly or by ment processes; procedures; and tation documents shall permit updating security controls as new threats / vulnerabilities and	reference, security requirements that describe the required:
Examine: Design system spec Examine: Pertinent policies an Interview: Programmer and p SA-4 – Acquisitions (High Control Security requirements and/or s with applicable laws, Executive Solicitation Documents Solicitation documents (e.g., F 4.15.4.1. Security capabilities; 4.15.4.2. Design and developr 4.15.4.3. Test and evaluation p 4.15.4.4. Documentation. The requirements in the solicit Use of Evaluated and Validate	cifications. nd procedures. programming supervisor.) security specifications shall be included, either explicitly or by reference, in all information e Orders, directives, policies, regulations, and standards. Request for Proposal) for any CMS information system shall include, either explicitly or by ment processes; procedures; and tation documents shall permit updating security controls as new threats / vulnerabilities and	re identified and as new technologies are implemented

products that have been evaluated and va	alidated through one or more of the following sources:			
 The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme; The International Common Criteria Recognition Arrangements; and The NIST Cryptographic Module Validation Program. 				
Configuration Settings and Implementatio The information system required docume	n Guidance ntation shall include security configuration settings, including documentation explaining e	exceptions to the standard, and security implementation guidance.		
Guidance				
capabilities (security needs and, as neces procedures; and (iv) required documentat	ts for Proposals) for information systems and services include, either explicitly or by refersary, specific security controls and other specific FISMA requirements); (ii) required desition. The requirements in the solicitation documents permit updating security controls as juidance on the selection of information security products. NIST SP 800-35 provides guictions in the system development life cycle.	ign and development processes; (iii) required test and evaluation new threats/vulnerabilities are identified and as new technologies are		
	ements for appropriate information system documentation. The documentation addresses rity controls in the information system. The level of detail required in the documentation is			
Use of Tested, Evaluated, and Validated NIST SP 800-23 provides guidance on the	Products e acquisition and use of tested/evaluated information technology products.			
Configuration Settings and Implementation				
	ntation includes security configuration settings and security implementation guidance. ON ems. NIST SP 800-70 provides guidance on configuration settings for information technol			
	ntation includes security configuration settings and security implementation guidance. ON ems. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4			
requirements for federal information syste	ems. NIST SP 800-70 provides guidance on configuration settings for information technol	logy products.		
requirements for federal information syste Applicability: All	ems. NIST SP 800-70 provides guidance on configuration settings for information technol	logy products.		
requirements for federal information syste Applicability: All ASSESSMENT PROCEDURE: SA-4.1	ems. NIST SP 800-70 provides guidance on configuration settings for information technol	logy products.		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security required accordance with applicable laws, Executive	References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 Irements and/or security specifications, either explicitly or by reference, in information system of or orders, directives, policies, regulations, and standards;	Related Controls:		
requirements for federal information syste Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requi accordance with applicable laws, Executiv (ii) the organization's acquisition of comm	ems. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irrements and/or security specifications, either explicitly or by reference, in information system we Orders, directives, policies, regulations, and standards; ercial information technology products is consistent with NIST SP 800-23;	Related Controls: stem acquisition contracts based on an assessment of risk and in		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requires accordance with applicable laws, Executive (ii) the organization's acquisition of common (iii) references to security configuration set	irements and/or security specifications, either explicitly or by reference, in information system of or orders, directives, policies, regulations, and standards; irection information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consistent	Related Controls: stem acquisition contracts based on an assessment of risk and in it with NIST SP 800-70; and		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinance with applicable laws, Executive (ii) the organization's acquisition of comme (iii) references to security configuration security is acquisition contracts for information security capabilities;	erns. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irements and/or security specifications, either explicitly or by reference, in information system ve Orders, directives, policies, regulations, and standards; ercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consisten systems include, either explicitly or by reference, security requirements and/or security specifications are consistent with specifications.	Related Controls: stem acquisition contracts based on an assessment of risk and in it with NIST SP 800-70; and		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinaccordance with applicable laws, Executin (ii) the organization's acquisition of commission of commission of commission of commission of commission of contracts for information system of the security configuration of the security configuration system of the security configuration system of the security configuration of the security configur	eres. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irrements and/or security specifications, either explicitly or by reference, in information system ve Orders, directives, policies, regulations, and standards; ercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consisten ystems include, either explicitly or by reference, security requirements and/or security spo sses;	Related Controls: stem acquisition contracts based on an assessment of risk and in it with NIST SP 800-70; and		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinaccordance with applicable laws, Executin (ii) the organization's acquisition of commination of commination of commination of commination of commination of contracts for information of commination of the organization contracts for information of the organization and development proces - required test and evaluation procedures	eres. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irrements and/or security specifications, either explicitly or by reference, in information system ve Orders, directives, policies, regulations, and standards; ercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consisten ystems include, either explicitly or by reference, security requirements and/or security spo sses;	Related Controls: stem acquisition contracts based on an assessment of risk and in it with NIST SP 800-70; and		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinaccordance with applicable laws, Executin (ii) the organization's acquisition of commination of commination of commination of commination of contracts for information of the organization contracts for information of the organization and development procedures in required test and evaluation procedures in required documentation.	eres. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irrements and/or security specifications, either explicitly or by reference, in information system ve Orders, directives, policies, regulations, and standards; ercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consisten ystems include, either explicitly or by reference, security requirements and/or security spo sses;	Related Controls: stem acquisition contracts based on an assessment of risk and in t with NIST SP 800-70; and		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinance with applicable laws, Executiv (ii) the organization's acquisition of commination of comminatin of commination of commination of comminati	ems. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irrements and/or security specifications, either explicitly or by reference, in information systems of orders, directives, policies, regulations, and standards; iercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consistent ystems include, either explicitly or by reference, security requirements and/or security spesses; ; and on policy; procedures addressing the integration of information security requirements and, acquisition contracts for information systems or services; other relevant documents or	Iogy products. Related Controls: stem acquisition contracts based on an assessment of risk and in at with NIST SP 800-70; and ecifications that describe: //or security specifications into the acquisition process; NIST SP 800-		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinaccordance with applicable laws, Executin (ii) the organization's acquisition of commination of co	ems. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irrements and/or security specifications, either explicitly or by reference, in information systems and/or security specifications, and standards; iercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consistent ystems include, either explicitly or by reference, security requirements and/or security specifications; sses; ; and	Iogy products. Related Controls: stem acquisition contracts based on an assessment of risk and in at with NIST SP 800-70; and ecifications that describe: //or security specifications into the acquisition process; NIST SP 800-		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinance with applicable laws, Executive (ii) the organization's acquisition of comme (iii) references to security configuration security configuration security configuration security capabilities; - required security capabilities; - required design and development proce - required test and evaluation procedures - required documentation. Assessment Methods And Objects Examine: System and services acquisition 23 and 800-70; acquisition documentation Interview: Organizational personnel with SA-4(1) – Enhancement (High)	ems. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irrements and/or security specifications, either explicitly or by reference, in information systems of orders, directives, policies, regulations, and standards; iercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consistent ystems include, either explicitly or by reference, security requirements and/or security spesses; ; and on policy; procedures addressing the integration of information security requirements and, acquisition contracts for information systems or services; other relevant documents or	Related Controls: stem acquisition contracts based on an assessment of risk and in at with NIST SP 800-70; and ecifications that describe: //or security specifications into the acquisition process; NIST SP 800-		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinated accordance with applicable laws, Executing (ii) the organization's acquisition of commination of acquisition contracts for information security capabilities; - required security capabilities; - required design and development procedures - required test and evaluation procedures - required documentation. Assessment Methods And Objects Examine: System and services acquisition 23 and 800-70; acquisition documentationr Interview: Organizational personnel with SA-4(1) – Enhancement (High) Control	ems. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irements and/or security specifications, either explicitly or by reference, in information system ve Orders, directives, policies, regulations, and standards; ercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consisten systems include, either explicitly or by reference, security requirements and/or security spe- sses; ; and on policy; procedures addressing the integration of information security requirements and n; acquisition contracts for information systems or services; other relevant documents or information system security, acquisition, and contracting responsibilities.	Item acquisition contracts based on an assessment of risk and in It with NIST SP 800-70; and ecifications that describe: I/or security specifications into the acquisition process; NIST SP 800-records.		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinated accordance with applicable laws, Executing (ii) the organization's acquisition of commination of acquisition contracts for information security capabilities; - required security capabilities; - required design and development procedures - required test and evaluation procedures - required documentation. Assessment Methods And Objects Examine: System and services acquisition 23 and 800-70; acquisition documentationr Interview: Organizational personnel with SA-4(1) – Enhancement (High) Control	ems. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irements and/or security specifications, either explicitly or by reference, in information systeve Orders, directives, policies, regulations, and standards; ercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consistent ystems include, either explicitly or by reference, security requirements and/or security specification of information security requirements and/or security specification of information security requirements and/or security specification of information security requirements and/or security specification contracts for information systems or services; other relevant documents or information system security, acquisition, and contracting responsibilities. t appropriate documentation be provided describing the functional properties of the secu	Independence Related Controls: Independence Related Controls: Independence Stem acquisition contracts based on an assessment of risk and in Int with NIST SP 800-70; and ecifications that describe: Interview Int with view NIST SP 800-70; and ecifications that describe: Int with view NIST SP 800-70; and ecifications that describe: Int with view NIST SP 800-70; and ecifications that describe: Int weight of the acquisition process; NIST SP 800-records. NIST SP 800-70; and ecifications into the acquisition process; NIST SP 800-records.		
requirements for federal information system Applicability: All ASSESSMENT PROCEDURE: SA-4.1 Assessment Objective Determine if: (i) the organization includes security requinaccordance with applicable laws, Executivi (ii) the organization's acquisition of commination of commination of commination of acquisition of commination of commination of acquisition contracts for information of equivalent equivalent of the organization of the organi	ems. NIST SP 800-70 provides guidance on configuration settings for information technol References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 irements and/or security specifications, either explicitly or by reference, in information systeve Orders, directives, policies, regulations, and standards; ercial information technology products is consistent with NIST SP 800-23; ettings and security implementation guidance in organizational acquisitions are consistent ystems include, either explicitly or by reference, security requirements and/or security specification of information security requirements and/or security specification of information security requirements and/or security specification of information security requirements and/or security specification contracts for information systems or services; other relevant documents or information system security, acquisition, and contracting responsibilities. t appropriate documentation be provided describing the functional properties of the secu	Iogy products. Related Controls: stem acquisition contracts based on an assessment of risk and in at with NIST SP 800-70; and ecifications that describe: I/or security specifications into the acquisition process; NIST SP 80 records.		

ASSESSMENT PROCEDURE: SA-4(1).1

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.

SA-4(CMS-1) – Enhancement (High)

Control

Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

Applicability: All	References: ARS: SA-4(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SA-4(CMS-1).1		

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records to determine that all contracts and Statements of Work (SOW) that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities to determine that all contracts and SOW that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

SA-5 – Information System Documentation (High)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

Guidance

Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Applicability: All	References: ARS: SA-5; FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1, TSD-3.1.2, TSD-3.1.3, TSP- 3.3.2; IRS-1075: 5.6.1.3#1.3; NIST 800-53/53A: SA-5; PISP: 4.15.5	Related Controls:

ASSESSMENT PROCEDURE: SA-5.1

Assessment Objective

Determine if:

(i) the organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system;

(ii) the organization makes available information on configuring, installing, and operating the information system; and

(iii) the organization makes available information on effectively using the security features in the information system.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; other relevant documents or records.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.

SA-5(1) – Enhancement (High) Control		
	on describes the functional properties of the security controls implemented within the information sy	stem with sufficient detail to facilitate analysis and testing of the
controls.		
Applicability: All	References: ARS: SA-5(1); NIST 800-53/53A: SA-5(1)	Related Controls:
ASSESSMENT PROCEDURE: S		
Assessment Objective		
	cludes, in addition to administrator and user guides, documentation, if available from the vendor/mar prmation system with sufficient detail to permit analysis and testing of the controls.	nufacturer, describing the functional properties of the security
Assessment Methods And Obje	ects	
	acquisition policy; procedures addressing information system documentation; information system de nnel with information system security, acquisition, and contracting responsibilities; organizational pe	
system.		soonnoi oporaang, asing, ana or mainaining tro mornation
SA-5(2) – Enhancement (High)		
Control		
Ensure that system documentati testing of the controls.	on describes the design and implementation details of the security controls implemented within the	information system with sufficient detail to permit analysis and
Applicability: All	References: ARS: SA-5(2); NIST 800-53/53A: SA-5(2)	Related Controls:
ASSESSMENT PROCEDURE: S		
Assessment Objective		
Determine if the organization inc security controls employed within	cludes, in addition to administrator and user guides, documentation, if available from the vendor/mar n the information system with sufficient detail to permit analysis and testing of the controls (including	
Determine if the organization inc security controls employed within Assessment Methods And Obje	n the information system with sufficient detail to permit analysis and testing of the controls (including ects	g functional interfaces among control components).
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system de	g functional interfaces among control components). esign documentation; other relevant documents or records.
Determine if the organization inc security controls employed withir Assessment Methods And Obje Examine: System and services Interview: Organizational person	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system de nnel with information system security documentation responsibilities; organizational personnel opera	g functional interfaces among control components). esign documentation; other relevant documents or records.
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (H	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system de nnel with information system security documentation responsibilities; organizational personnel opera	g functional interfaces among control components). esign documentation; other relevant documents or records.
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (H Control	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system de nnel with information system security documentation responsibilities; organizational personnel opera High)	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system.
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (H Control Develop system documentation f	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system de nnel with information system security documentation responsibilities; organizational personnel oper High to describe the system and to specify the purpose, technical operation, access, maintenance, and re	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users.
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (H Control Develop system documentation f Applicability: All	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system do nnel with information system security documentation responsibilities; organizational personnel opera- tigh) to describe the system and to specify the purpose, technical operation, access, maintenance, and re References: ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system.
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (F Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system do nnel with information system security documentation responsibilities; organizational personnel opera- tigh) to describe the system and to specify the purpose, technical operation, access, maintenance, and re References: ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users.
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (F Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system do nnel with information system security documentation responsibilities; organizational personnel opera High) to describe the system and to specify the purpose, technical operation, access, maintenance, and r References: ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1 SA-5(CMS-1).1	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls:
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (F Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc security controls employed within	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system de nnel with information system security documentation responsibilities; organizational personnel opera High) to describe the system and to specify the purpose, technical operation, access, maintenance, and r References: ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1 SA-5(CMS-1).1	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls:
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (F Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system do nnel with information system security documentation responsibilities; organizational personnel opera High) to describe the system and to specify the purpose, technical operation, access, maintenance, and r References: ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1 SA-5(CMS-1).1 cludes, in addition to administrator and user guides, documentation, if available from the vendor/mar n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing the requirements for information system documentation; i	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls: hufacturer, describing the design and implementation details of the g functional interfaces among control components).
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (F Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a guides; other relevant document	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system do nnel with information system security documentation responsibilities; organizational personnel opera High) to describe the system and to specify the purpose, technical operation, access, maintenance, and re References: ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1 SA-5(CMS-1).1	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls: hufacturer, describing the design and implementation details of the g functional interfaces among control components).
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (H Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a guides; other relevant document maintenance; and required person Interview: Organizational person	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system detail to describe the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system and to specify the purpose, technical operation, access, maintenance, and receive the system system and to specify the purpose, technical operation, access, maintenance, and receive the system security access, acc	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls: nufacturer, describing the design and implementation details of the g functional interfaces among control components). information system documentation including administrator and user s purpose; description; technical operations and access; ing, and/or maintaining the information system to determine the
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (H Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a guides; other relevant document maintenance; and required person Interview: Organizational person organization develops system do and users.	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system detail to describe the system and to specify the purpose, technical operation, access, maintenance, and recess in addition to administrator and user guides, documentation, if available from the vendor/mar in the information system with sufficient detail to permit analysis and testing of the controls (including ects) acquisition policy; procedures addressing the requirements for information system documentation; is or records to determine the organization develops system documentation to describe the system and users. Innel with information system documentation; is or records to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance, use of the formation system documentation is provide administrators and users.	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls: nufacturer, describing the design and implementation details of the g functional interfaces among control components). information system documentation including administrator and user s purpose; description; technical operations and access; ing, and/or maintaining the information system to determine the
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (H Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a guides; other relevant document maintenance; and required person Interview: Organizational person organization develops system do and users.	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system detail to describe the system and to specify the purpose, technical operation, access, maintenance, and recess in addition to administrator and user guides, documentation, if available from the vendor/mar in the information system with sufficient detail to permit analysis and testing of the controls (including ects) acquisition policy; procedures addressing the requirements for information system documentation; is or records to determine the organization develops system documentation to describe the system and users. Innel with information system documentation; is or records to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance, use of the formation system documentation is provide administrators and users.	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls: nufacturer, describing the design and implementation details of the g functional interfaces among control components). information system documentation including administrator and use s purpose; description; technical operations and access; ing, and/or maintaining the information system to determine the
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (H Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a guides; other relevant document maintenance; and required person organization develops system do	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system detail to describe the system and to specify the purpose, technical operation, access, maintenance, and recess in addition to administrator and user guides, documentation, if available from the vendor/mar in the information system with sufficient detail to permit analysis and testing of the controls (including ects) acquisition policy; procedures addressing the requirements for information system documentation; is or records to determine the organization develops system documentation to describe the system and users. Innel with information system documentation; is or records to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance, use of the formation system documentation is provide administrators and users.	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls: nufacturer, describing the design and implementation details of the g functional interfaces among control components). information system documentation including administrator and user s purpose; description; technical operations and access; ing, and/or maintaining the information system to determine the
Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a Interview: Organizational person SA-5(CMS-1) – Enhancement (F Control Develop system documentation f Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if the organization inc security controls employed within Assessment Methods And Obje Examine: System and services a guides; other relevant document maintenance; and required person organization develops system do and users. SA-5(CMS-2) – Enhancement (F Control	n the information system with sufficient detail to permit analysis and testing of the controls (including ects acquisition policy; procedures addressing information system documentation; information system detail to describe the system and to specify the purpose, technical operation, access, maintenance, and recess in addition to administrator and user guides, documentation, if available from the vendor/mar in the information system with sufficient detail to permit analysis and testing of the controls (including ects) acquisition policy; procedures addressing the requirements for information system documentation; is or records to determine the organization develops system documentation to describe the system and users. Innel with information system documentation; is or records to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance, use of the formation system documentation is provide administrators and users.	g functional interfaces among control components). esign documentation; other relevant documents or records. ating, using, and/or maintaining the information system. equired training for administrators and users. Related Controls: nufacturer, describing the design and implementation details of the g functional interfaces among control components). information system documentation including administrator and user s purpose; description; technical operations and access; ing, and/or maintaining the information system to determine the

ASSESSMENT PROCEDURE: SA-5(CMS-2).1		
Assessment Objective		
	n to administrator and user guides, documentation, if available from the vendor/manufacturer, describ n system with sufficient detail to permit analysis and testing of the controls (including functional interfa	
Assessment Methods And Objects		
	y; procedures addressing the requirements for information system documentation; information system tetermine the organization maintains an updated list of related system's operations and security docured and s	
organization maintains an updated list of related	ation system documentation responsibilities; organizational personnel operating, using, and/or mainta system's operations and security documentation.	ining the information system to determine the
SA-5(CMS-3) – Enhancement (High)		
Control		
Update documentation upon changes in system security of hard copies depending on data sensit		. Refer to "Media Protection" standard for
Applicability: All	References: ARS: SA-5(CMS-3); FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1	Related Controls:
ASSESSMENT PROCEDURE: SA-5(CMS-3).1		
Assessment Objective		
Determine if responsible parties within the organ	ization periodically review system and services acquisition policy and procedures.	
Assessment Methods And Objects		
Examine: System and services acquisition polic	y; procedures addressing the requirements for information system documentation; information system	documentation including administrator and user
	letermine the organization updates documentation upon changes in system functions and processes.	
	Protection" standard for security of hard copies depending on data sensitivity included in the documen	
	ation system documentation responsibilities; organizational personnel operating, using, and/or mainta	
standard for security of hard copies depending o	ges in system functions and processes. Must include date and version number on all formal system d	ocumentation. Refer to "Media Protection"
SA-5(CMS-4) – Enhancement (High)		
Control		
	dures in support of system access administration and operations.	
Applicability: All	References: ARS: SA-5(CMS-4); FISCAM: TSD-1.1.6	Related Controls:
ASSESSMENT PROCEDURE: SA-5(CMS-4).1		·
Assessment Objective		
Determine if the organization includes, in additio	n to administrator and user guides, documentation, if available from the vendor/manufacturer, describ n system with sufficient detail to permit analysis and testing of the controls (including functional interfa	
Assessment Methods And Objects		
	y; procedures addressing the requirements for information system documentation; information system	
	letermine the organization documents the system's configuration and procedures in support of system	
	ation system documentation responsibilities; organizational personnel operating, using, and/or mainta	ining the information system to determine the
	on and procedures in support of system access administration and operations.	
SA-5(FIS-1) – Enhancement (High)		
Control		
Goals are established by senior management or		
with the goals and surveys user departments to		· · ·
with the goals and surveys user departments to a Applicability: All		d compares the service performance achieved Related Controls:
with the goals and surveys user departments to	see if their needs are being met.	· · ·
with the goals and surveys user departments to a Applicability: All	see if their needs are being met.	· · ·
with the goals and surveys user departments to a Applicability: All ASSESSMENT PROCEDURE: SA-5(FIS-1).1 Assessment Objective Determine if the organizational goals are establis	see if their needs are being met.	Related Controls:

Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation.		
Interview: Senior management, data processing	g management, and user management.	
SA-5(FIS-2) – Enhancement (High)		
Control		
Records are maintained on the actual performar identify recurring patterns or trends.	nce in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time f	or resolution are recorded and analyzed to
Applicability: All	References: FISCAM: TSC-2.4.7, TSC-2.4.8	Related Controls:
ASSESSMENT PROCEDURE: SA-5(FIS-2).1		
Assessment Objective Determine if the organizational records are main recorded and analyzed to identify recurring patter	tained on the actual performance in meeting service schedules. Problems and delays encountered, the r erns or trends.	reason, and the elapsed time for resolution are
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation.		
Interview: Senior management, data processing		
SA-6 – Software Usage Restrictions (Hi	gh)	
Control		
license agreement shall be prohibited. The use unauthorized distribution, display, performance, Guidance	y quantity licenses shall be managed through a tracking system to control copying and distribution. All o of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure or reproduction of copyrighted work.	that this capability is not used for the
Software and associated documentation are use organization employs tracking systems to contro	ed in accordance with contract agreements and copyright laws. For software and associated documentati I copying and distribution. The organization controls and documents the use of publicly accessible peer-tistribution, display, performance, or reproduction of copyrighted work.	on protected by quantity licenses, the to-peer file sharing technology to ensure that
Applicability: All	References: ARS: SA-6; FISCAM: TCC-2.3.1; IRS-1075: 4.7.3#1.2; NIST 800-53/53A: SA-6; PISP: 4.15.6	Related Controls:
ASSESSMENT PROCEDURE: SA-6.1		•
Assessment Objective		
Determine if:		
(i) the organization complies with software usage		
 (ii) the organization regularly reviews/analyzes s appropriate officials, and takes necessary action 	oftware usage for indications of inappropriate or unusual activity, investigates suspicious activity or susp s.	ected violations, reports findings to
Assessment Methods And Objects		
records.	y; procedures addressing software usage restrictions; site license documentation; list of software usage	
	ation system administration responsibilities; organizational personnel operating, using, and/or maintainin	g the information system.
SA-6(FIS-1) – Enhancement (High)		
Control		
Implementation orders, including effective date,	are provided to all locations where they are maintained on file.	1
Applicability: All	References: FISCAM: TCC-2.3.2	Related Controls:
ASSESSMENT PROCEDURE: SA-6(FIS-1).1		
Assessment Objective		

Assessment Methods And Objects Examine: Implementation orders. Examine: Pertinent policies and procedures. Interview: Information system and security administrators. SA-7 – User Installed Software (High) Control All users shall be restricted from downloading or installing software, unless explicitly authorized in writing by the CIO or his/her designated representative. Users that have been granted such authorization may download and install only organization-approved software. The use of install-on-demand software shall be restricted. Guidance If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect) Applicability: All References: ARS: SA-7; FISCAM: TCC-1.3.1; NIST 800-53/53A: SA-7; PISP: 4.15.7 **Related Controls: ASSESSMENT PROCEDURE: SA-7.1 Assessment Objective** Determine if: (i) the organization enforces explicit rules governing the installation of software by users; (ii) unauthorized software is present on the system; and (iii) the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary action. **Assessment Methods And Objects** Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records. Interview: Organizational personnel with information system administration responsibilities: organizational personnel operating, using, and/or maintaining the information system. Test: Enforcement of rules for user installed software on the information system: information system for prohibited software. SA-7(CMS-1) – Enhancement (High) Control If user installed software is authorized in writing by the CIO or his/her designated representative, ensure that business rules and technical controls enforce the documented authorizations and prohibitions. Applicability: All References: ARS: SA-7(CMS-1) **Related Controls:** ASSESSMENT PROCEDURE: SA-7(CMS-1).1 **Assessment Objective** Determine if: (i) the organization enforces explicit rules governing the installation of software by users; and (ii) unauthorized software is present on the system. Assessment Methods And Objects Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records to determine that policies exist that ensure business rules and technical controls enforce the documented authorizations and prohibitions. Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine that policies exist that ensure business rules and technical controls enforce the documented authorizations and prohibitions. Test: Enforcement of rules for user installed software on the information system; information system for prohibited software to determine authorizations and prohibitions. SA-8 – Security Engineering Principles (High) Control CMS information systems shall be designed and implemented using accepted security engineering principles. Guidance NIST SP 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to

system upgrades and modifications, to the exten	t feasible, given the current state of the hardware, software, and firmware components within the system	I.			
Applicability: All	References: ARS: SA-8; FISCAM: TAY-2.1.1, TAY-2.2.1, TCC-2.1.3; NIST 800-53/53A: SA-8; PISP: 4.15.8	Related Controls:			
ASSESSMENT PROCEDURE: SA-8.1					
Assessment Objective					
Determine if:					
	information system using security engineering principles; and	-			
	nciples in the development and implementation of the information system consistent with NIST SP 800-2	27.			
	Assessment Methods And Objects Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST SP 800-27;				
information system design documentation: secur	ity requirements and security specifications for the information system; other relevant documents or reco	r the information system, NIST SP 800-27; ords			
Interview: Organizational personnel with system					
SA-8(0) – Enhancement (High)					
Control					
	sing the security engineering principles detailed in NIST SP 800-27 Rev. A, Engineering Principles for IT	Security (A Baseline for Achieving Security).			
Applicability: All	References: ARS: SA-8(0); FISCAM: TCC-2.1.3; NIST 800-53/53A: SA-8; PISP: 4.15.8	Related Controls:			
ASSESSMENT PROCEDURE: SA-8(0).1					
Assessment Objective					
	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ving enhancement to the baseline control.			
Assessment Methods And Objects					
	y; procedures addressing security engineering principles used in the development and implementation o				
	ity requirements and security specifications for the information system; other relevant documents or reco	ords.			
Interview: Organizational personnel with system					
SA-9 – External Information System Ser	vices (High)				
Control					
	lude specific provisions requiring the service provider to comply with CMS IS policies, standards, and gu				
	any loss, disruption, or damage caused by the service provider's failure to comply. Service providers sha n writing, by the CMS CIO or his/her designated representatives with concurrence from CMS' personnel				
Guidance					
	ce that is implemented outside of the accreditation boundary of the organizational information system (i.	e, a service that is used by, but not a part of			
	ships with external service providers are established in a variety of ways, for example, through joint vent				
	cy agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges.				
	and assets, and to individuals, arising from the use of external information system services remains with				
	e established with external service providers when dealing with the many issues associated with informate e organization establish and retain a level of confidence that each participating service provider in the po				
	services rendered to the organization. Where a sufficient level of trust cannot be established in the exte				
	trols or accepts the greater degree of risk to its operations and assets, or to individuals. The external infi				
includes government, service provider, and end	user security roles and responsibilities, and any service-level agreements. Service-level agreements def	ne the expectations of performance for each			
required security control, describe measurable o	utcomes, and identify remedies and response requirements for any identified instance of non-compliance	e. NIST SP 800-35 provides guidance on			
	P 800-64 provides guidance on the security considerations in the system development life cycle.	Deleted Originals, OA 0			
Applicability: All	References: ARS: SA-9; FISCAM: TAY-1.3.1; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4; NIST 800-53/53A: SA-9; PISP: 4.15.9	Related Controls: CA-3			
ASSESSMENT PROCEDURE: SA-9.1		1			
Assessment Objective					
Determine if:					
	(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies,				
regulations, standards, guidance, and establishe					
(ii) the organization monitors security control con	npliance;				

	views/analyzes outsourced information system services for indications of inappropriate or unusual activity, inve	estigates suspicious activity or suspected violations,
, , , , ,	ficials, and takes necessary actions; and ed by providers of external information system services are compliant with applicable federal laws, directives,	policies, regulations, standards, guidance, and
established service level agreem		
Assessment Methods And Obje		
	acquisition policy; procedures addressing external information system services; acquisition contracts and serv	
records.	ications for external provider services; security control assessment evidence from external providers of inform	nation system services; other relevant documents or
	nnel with system and services acquisition responsibilities; external providers of information system services.	
SA-9(CMS-1) – Enhancement (H	ligh)	
Control		
	ed in writing by the CMS CIO or his/her designated representative to outsource any system function overseas, scribe measurable outcomes, and identify remedies and response requirements for any identified instance of	
Applicability: All	References: ARS: SA-9(CMS-1): HIPAA: 164.314(b)(2)(iiii): HSPD 7: D(8)	Related Controls:
ASSESSMENT PROCEDURE: S		
Assessment Objective		
Determine if the organization req policies, regulations, standards, g	uires that providers of external information system services employ adequate security controls in accordance guidance, and established service-level agreements.	with applicable laws, Executive Orders, directives,
Assessment Methods And Obje	ects	
requirements and security specif records to determine that service of non-compliance for service pro Interview: Organizational persor expectations of performance, det	acquisition policy; procedures addressing external information system services; acquisition contracts and serv ications for external provider services; security control assessment evidence from external providers of inform e level agreements define expectations of performance, describe measurable outcomes, and identify remedie: oviders who are authorized in writing by the CMS CIO or his/her designated representative to outsource any services to scribe measurable outcomes, and identify remedies and response requirements for any identified instance of /her designated representative to outsource any system function overseas.	nation system services; other relevant documents or s and response requirements for any identified instance system function overseas.
SA-9(HIP-1) – Enhancement (Hi		
Control	5··/	
A covered entity under HIPAA ma	ay permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf or ations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (Se	
Applicability: All	References: HIPAA: 164.308(b)(1), 164.308(b)(4), 164.314(a)(1)(i), 164.314(a)(2)(i), 164.314(a)(2)(i), 164.314(a)(2)(i)(B), 164.314(a)(2)(i)(C), 164.314(a)(2)(i)(D), 164.314(a)(2)(ii)(A)(1), 164.314(a)(2)(ii)(A)(2), 164.314(a)(2)(ii)(B)	Related Controls:
ASSESSMENT PROCEDURE: S	A-9(HIP-1).1	
Assessment Objective		
	overed entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements se	
Assessment Methods And Obje	ects	
Examine: Organizational docum	entation meets the requirements set forth in HIPAA regulations (See HIPAA 164.308(b) and 164.314(a)) for a	a covered entity.
Interview: Organizational persor	nnel maintaining covered entity documentation follow requirements set forth in HIPAA regulations. (See HIPA	A 164.308(b) and 164.314(a).)
SA-10 – Developer Configura	ation Management (High)	
Control		
	hall develop, document, and implement a configuration management plan for each information system under isms during development, change authorization requirements, and security flaw identification, tracking, and re	
Guidance		
This control also applies to the de	evelopment actions associated with information system changes.	
Applicability: All	References: ARS: SA-10; NIST 800-53/53A: SA-10; PISP: 4.15.10	Related Controls:
Der 0	$P_{0} = 162 = f_{0} 207$	DDCCM Amondia A Attachment 1

ASSESSMENT PROCEDURE: SA-10.1		
Assessment Objective		
-	formation system developers (and systems integrators) create and implement a con	figuration management plan that controls changes to the system
during development, tracks security flaws, re	equires authorization of changes, and provides documentation of the plan and its imp	plementation.
Assessment Methods And Objects		
Examine: System and services acquisition	policy; procedures addressing information system developer/integrator configuration	management; acquisition contracts and service level agreements;
information system developer/integrator con	figuration management plan; security flaw tracking records; system change authorize	ation records; other relevant documents or records.
SA-11 – Developer Security Testing	(High)	
Control		
Information system developers shall develop	o, document, and implement a security test and evaluation (ST&E) plan for each info	rmation system under development in accordance with, but not limited
	oper security test results shall be documented.	
Guidance	· · · ·	
Developmental security test results are used	I to the greatest extent feasible after verification of the results and recognizing that the	hese results are impacted whenever there have been security relevan
	equent to developer testing. Test results may be used in support of the security cert	
system.		
Applicability: All	References: FISCAM: TCC-2.1.5; NIST 800-53/53A: SA-11	Related Controls: CA-2, CA-4
ASSESSMENT PROCEDURE: SA-11.1		
Assessment Objective		
Determine if the organization requires that in	formation system developers (and systems integrators) create a security test and ev	valuation plan, implement the plan, and document the results.
Assessment Methods And Objects		
•	oolicy; procedures addressing information system developer/integrator security testir	ng: acquisition contracts and service level agreements: information
	ns; records of developer/integrator security testing results for the information system	
SA-11(CMS-1) – Enhancement (High)		
Control		
	esults are used in support of the security C&A process for the information system, er	nsure that no security relevant modifications of the information
	security testing and after selective verification of the results.	
Applicability: All	References: ARS: SA-11(CMS-1); FISCAM: TCC-2.1.8	Related Controls:
ASSESSMENT PROCEDURE: SA-11(CMS		
Assessment Objective		
	formation system developers (and systems integrators) create a security test and ev	valuation plan implement the plan and document the results
Assessment Methods And Objects		
	policy; procedures addressing information system developer/integrator security testir	on: acquisition contracts and service level agreements: information
system developer/integrator security test pla	ns; records of developer/integrator security testing results for the information system	n: other relevant documents or records to determine that no security
	tem has been made subsequent to the security testing and after selective verification	
support of the security C&A process for the		· · · · · · · · · · · · · · · · · · ·
Interview: Organizational personnel with de	veloper security testing responsibilities to determine that no security relevant modific	cations of the information system has been made subsequent to the
security testing and after selective verification	n of the results if the security test and evaluation results are used in support of the s	security C&A process for the information system.
SA-11(CMS-2) – Enhancement (High)		
Control		
Use hypothetical data when executing test s	cripts.	
Applicability: All	References:	Related Controls:
ASSESSMENT PROCEDURE: SA-11(CMS	-2).1	
Assessment Objective		
	ccess to areas officially designated as publicly accessible, as appropriate, in accord	ance with the organization's assessment of risk.
Assessment Methods And Objects		
	policy; procedures addressing software and information integrity; information system	design documentation: information system configuration settings and
Examine. Oystern and information integrity	solidy, procedures addressing soliware and mornation integrity, mornation system	accign accumentation, information system configuration settings and

Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records to determine hypothetical data is used when executing test scripts.

ASSESSMENT DROCEDURE, SA 10.1

Interview: Personnel with system and information integrity responsibilities to determine hypothetical data is used when executing test scripts. **Test:** Information systems to determine hypothetical data is used when executing test scripts.

System and Communications Protection (SC) – *Technical*

SC-1 – System and Communications Protection Policy and Procedures (High)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: SC-1; FISCAM: TAC-3.2.E.1; IRS-1075: 5.6.3.4#1, 5.6.3.4#2; NIST 800-53/53A: SC-1; PISP: 4.16.1	Related Controls:

ASSESSMENT PROCEDURE: SC-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents system and communications protection policy and procedures;

(ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and

(iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and communications protection responsibilities.

ASSESSMENT PROCEDURE: SC-1.2

Assessment Objective

Determine if:

(i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and communications protection responsibilities.

SC-2 – Application Partitioning (High)

Control

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Guidance

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Applicability: All	References: ARS: SC-2; NIST 800-53/53A: SC-2; PISP: 4.16.2	Related Controls:
ASSESSMENT PROCEDURE: SC-2.1		

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Separation of user functionality from information system management functionality.

SC-2(CMS-1) – Enhancement (High)

Control

Place all CMS servers allowing public access within a DMZ environment, and disallow direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Applicability: All	References: ARS: SC-2(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SC-2(CMS-1).1		

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Interview: Selected organizational personnel with network administration responsibilities to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers. Test: All CMS servers allowing public access to the internal network. DMZ servers can only access these servers within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

SC-3 – Security Function Isolation (High)

Control

Information system security functions shall be isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system shall maintain a separate execution domain (e.g., address space) for each executing process.

Guidance

The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Applicability: All	References: ARS: SC-3; NIST 800-53/53A: SC-3; PISP: 4.16.3	Related Controls:
AGGEGGMENT PROGEDURE: 00 24		

ASSESSMENT PROCEDURE: SC-3.1

Assessment Objective

Determine if:

(i) the organization defines the security functions of the information system to be isolated from nonsecurity functions; and

(ii) the information system isolates security functions from nonsecurity functions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Separation of security functions from nonsecurity functions within the information system.

SC-3(1) – Enhancement (High)

Control

Employ hardware separation mechanisms to facilitate the isolation of security functions.

Applicability: All	References: ARS: SC-3(1); NIST 800-53/53A: SC-3(1)	Related Controls:
ASSESSMENT PROCEDURE: SC-3(1).1		

Assessment Objective

Determine if the information system employs underlying hardware separation mechanisms to facilitate security function isolation.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; hardware separation mechanisms; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Hardware separation mechanisms facilitat	ting security function isolation.(Optional)	
SC-3(2) – Enhancement (High)		
Control		
Isolate critical security functions from both non-		
Applicability: All	References: ARS: SC-3(2); NIST 800-53/53A: SC-3(2)	Related Controls:
ASSESSMENT PROCEDURE: SC-3(2).1		
Assessment Objective		
Determine if:		
() C	unctions of the information system to be isolated from both nonsecurity functions and from other securit	y functions; and
	ty functions from both nonsecurity functions and from other security functions.	
Assessment Methods And Objects	and a barrent of the second	
system configuration settings and associated do	on policy; procedures addressing security function isolation; list of critical security functions; information ocumentation; other relevant documents or records.(Optional)	n system design documentation; information
Test: Isolation of critical security functions.(Opti	onal)	
SC-3(3) – Enhancement (High)		
Control		
	ncluded within the isolation boundary containing security functions.	
Applicability: All	References: ARS: SC-3(3); NIST 800-53/53A: SC-3(3)	Related Controls:
ASSESSMENT PROCEDURE: SC-3(3).1		
Assessment Objective		
	he number of nonsecurity functions included within the isolation boundary containing security functions	
Assessment Methods And Objects		
	on policy; procedures addressing security function isolation; information system design documentation	information system configuration settings and
associated documentation; other relevant docur	nents or records.(Optional)	
SC-3(4) – Enhancement (High)		
Control		
	dent modules that avoid unnecessary interactions between modules.	
Applicability: All	References: ARS: SC-3(4); NIST 800-53/53A: SC-3(4)	Related Controls:
ASSESSMENT PROCEDURE: SC-3(4).1		
Assessment Objective		
	ctions are implemented as largely independent modules that avoid unnecessary interactions between i	modules.
Assessment Methods And Objects		
	on policy; procedures addressing security function isolation; information system design documentation	information system configuration settings and
associated documentation; other relevant docur	nents or records.(Optional)	
SC-3(5) – Enhancement (High)		
Control		
	are minimizing interactions between layers of the design and avoiding any dependence by lower layers	on the functionality or correctness of higher
layers.		
	References: ARS: SC-3(5); NIST 800-53/53A: SC-3(5)	Related Controls:
ASSESSMENT PROCEDURE: SC-3(5).1		
Assessment Objective		
the functionality or correctness of higher layers.	ctions are implemented as a layered structure minimizing interactions between layers of the design and	d avoiding any dependence by lower layers on
Assessment Methods And Objects		
Examine: System and communications protecti associated documentation; other relevant docur	on policy; procedures addressing security function isolation; information system design documentation nents or records.(Optional)	information system configuration settings and
Rev. 9	Page 168 of 207	BPSSM Appendix A, Attachment 1

SC-4 – Information Remnance	(High)	
Control		
No information, including encrypted i	representations of information, produced by a prior user's actions (or the actions is access to a shared system resource that has been released back to the inform	
Guidance		
Control of information system remna of a prior user/role (or the actions of		ation, including encrypted representations of information, produced by the actions ent user/role (or current process) that obtains access to a shared system resource tem.
Applicability: All	References: ARS: SC-4; IRS-1075: 5.6.3.4#2, 5.6.3.4#3; NIST 80	
ASSESSMENT PROCEDURE: SC-4		
Assessment Objective		
	prevents unauthorized and unintended information transfer via shared system re	esources
Assessment Methods And Objects	,	
	ons protection policy; procedures addressing information remnance; information	system design documentation; information system configuration settings and
	orized and unintended transfer of information via shared system resources.	
SC-4(0) – Enhancement (High)		
Control		
Ensure that users of shared system	resources cannot intentionally or unintentionally access information remnants, ir on behalf of a prior user. Ensure that system resources shared between two (2) sure.	
Applicability: All	References: ARS: SC-4(0); IRS-1075: 5.6.3.4#2; NIST 800-53/53	A: SC-4; PISP: 4.16.4 Related Controls:
ASSESSMENT PROCEDURE: SC-4		
Assessment Objective Determine if the organization meets Assessment Methods And Objects	the requirements as specified in the baseline control and the specific CMS requ	irements as prescribed in this amplifying enhancement to the baseline control.
	ons protection policy; procedures addressing information remnance; information	system design documentation; information system configuration settings and
	orized and unintended transfer of information via shared system resources.	
SC-4(PII-1) – Enhancement (High)		
Control		
For PII, when authorized to make fur disclosure was made, what was disc	closed, and why and when it was disclosed. Organizations transmitting PII from o	side the organization must be recorded on a separate list that reflects to whom th one computer to another need only identify the bulk records transmitted. This ole description of the records, and the name of the individual making/receiving the
Applicability: All	References: IRS-1075: 3.3#2	Related Controls:
ASSESSMENT PROCEDURE: SC-4	4(PII-1).1	
Assessment Objective		
Determine if the organization determ reflects to whom the disclosure was	nines authorizations for further disclosures (e.g., agents/contractors), information made, what was disclosed, and why and when it was disclosed. Organizations to ontain the approximate number of personal records, the date of the transmission	transmitting PII from one computer to another need only identify the bulk records
Assessment Methods And Objects	5	
•	ch have been transmitted externally to another organization to determine if the re	ecords contain:

- date of the transmission
- best possible description of the records

 the name of the individuals making/receiving the 	e transmission.		
SC-5 – Denial of Service Protection (High	h)		
Control			
	imit the effects of well-known, detectable, and preventable denial-of-service attacks.		
Guidance			
	e cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can	filter certain types of packets to protect	
	m being directly affected by denial of service attacks. Information systems that are publicly accessible ca		
capacity and bandwidth combined with service re	edundancy.		
Applicability: All	References: ARS: SC-5; NIST 800-53/53A: SC-5; PISP: 4.16.5	Related Controls:	
ASSESSMENT PROCEDURE: SC-5.1			
Assessment Objective			
Determine if:			
	service attacks (or provides references to sources of current denial of service attacks) that can be addre	essed by the information system; and	
	its the effects of the organization-defined or referenced types of denial of service attacks.		
Assessment Methods And Objects			
	on policy; procedures addressing denial of service protection; information system design documentation;	information system security plan; information	
	cumentation; other relevant documents or records.		
· · · ·	r limitation of the effects of denial of service attacks.		
SC-5(0) – Enhancement (High)			
Control			
	I-of-service attacks defined on the following sites or within the following documents:		
- SANS Organization www.sans.org/dosstep;			
 SANS Organization's Roadmap to Defeating D NIST CVE List http://checklists.nist.gov/home.c 			
Applicability: All	References: ARS: SC-5(0); NIST 800-53/53A: SC-5; PISP: 4.16.5	Related Controls:	
ASSESSMENT PROCEDURE: SC-5(0).1	Release ANS. 50-5(0), NOT 500-55(55A. 50-5, 1151. 4.10.5	Related Controls.	
Assessment Objective	ante en encificad in the baseline control and the encodin CMC new instructs on anomibed in this encodi	in a sub-supervised to the baseline sector.	
o 1	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ling enhancement to the baseline control.	
Assessment Methods And Objects	e estimate and the size denies of service material information systems denies denies de sur stations	information and a construction (for list of	
	 policy; procedures addressing denial of service protection; information system design documentation; tacks to protect against or limit); information system configuration settings and associated documentatio 		
	r limitation of the effects of denial of service attacks.	n, other relevant documents of records.	
SC-5(1) – Enhancement (High)			
Control			
Control	ruice attacke against other information quaterns or natuorke		
Restrict the ability of users to launch denial of se	rvice attacks against other information systems or networks.	Polated Controls	
Restrict the ability of users to launch denial of se Applicability: All	rvice attacks against other information systems or networks. References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1)	Related Controls:	
Restrict the ability of users to launch denial of se Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1		Related Controls:	
Restrict the ability of users to launch denial of se Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1 Assessment Objective	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1)	Related Controls:	
Restrict the ability of users to launch denial of se Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1 Assessment Objective Determine if the information system restricts the		Related Controls:	
Restrict the ability of users to launch denial of se Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1 Assessment Objective Determine if the information system restricts the Assessment Methods And Objects	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1) ability of users to launch denial of service attacks against other information systems or networks.		
Restrict the ability of users to launch denial of se Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1 Assessment Objective Determine if the information system restricts the Assessment Methods And Objects Examine: System and communications protection	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1) ability of users to launch denial of service attacks against other information systems or networks.		
Restrict the ability of users to launch denial of set Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1 Assessment Objective Determine if the information system restricts the Assessment Methods And Objects Examine: System and communications protection associated documentation; other relevant docum	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1) ability of users to launch denial of service attacks against other information systems or networks. on policy; procedures addressing denial of service protection; information system design documentation; ients or records].(Optional)		
Restrict the ability of users to launch denial of set Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1 Assessment Objective Determine if the information system restricts the Assessment Methods And Objects Examine: System and communications protection associated documentation; other relevant docum Test: Information system for protection against of	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1) ability of users to launch denial of service attacks against other information systems or networks.		
Restrict the ability of users to launch denial of set Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1 Assessment Objective Determine if the information system restricts the Assessment Methods And Objects Examine: System and communications protection associated documentation; other relevant docum Test: Information system for protection against of SC-5(2) – Enhancement (High)	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1) ability of users to launch denial of service attacks against other information systems or networks. on policy; procedures addressing denial of service protection; information system design documentation; ients or records].(Optional)		
Restrict the ability of users to launch denial of set Applicability: All ASSESSMENT PROCEDURE: SC-5(1).1 Assessment Objective Determine if the information system restricts the Assessment Methods And Objects Examine: System and communications protection associated documentation; other relevant docum Test: Information system for protection against of SC-5(2) – Enhancement (High) Control	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1) ability of users to launch denial of service attacks against other information systems or networks. on policy; procedures addressing denial of service protection; information system design documentation; ients or records].(Optional)		

Applicability: All	References: ARS: SC-5(2); NIST 800-53/53A: SC-5(2)	Related Controls:
ASSESSMENT PROCEDURE: SC-5(2).1		•
Assessment Objective		
-	s excess capacity, bandwidth, or other redundancy to limit the effects of information flood	ling types of denial of service attacks.
Assessment Methods And Objects		
Examine: System and communications prote associated documentation; other relevant do	ection policy; procedures addressing denial of service protection; information system desi ocuments or records].(Optional)	ign documentation; information system configuration settings and
SC-6 – Resource Priority (High)		
Control		
Mechanisms shall be implemented to provide with the information system servicing any hig	e for allocation of information system resources based upon priority. Priority protection sh gher-priority process.	hall ensure that a lower-priority process is not able to interfere
Guidance		
	rity process from delaying or interfering with the information system servicing any higher-p	
Applicability: All	References: ARS: SC-6; FISCAM: TSC-1.1; NIST 800-53/53A: SC-6; PISP: 4.16.6	Related Controls:
ASSESSMENT PROCEDURE: SC-6.1		
Assessment Objective		
Determine if the information system limits the	e use of resources by priority.	
Assessment Methods And Objects		
	ection policy; procedures addressing prioritization of information system resources; inform	nation system design documentation; information system
	nentation; other relevant documents or records.(Optional)	
SC-7 – Boundary Protection (High)		
Control		
the external boundary of the information syst	s shall be established and supporting procedures shall be developed, documented, and in tem and at key internal boundaries within the system. Any connections to the Internet, or	nplemented effectively to monitor and control communications at other external networks or information systems, shall occur
		ase of information outside of the information system boundary.
Information system boundary protections at a	al failure of the boundary protection mechanisms shall not result in any unauthorized relea any designated alternate processing site shall provide the same levels of protection as the	ase of information outside of the information system boundary.
Information system boundary protections at a Guidance Any connections to the Internet, or other exter routers, firewalls, guards, encrypted tunnels)		ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred to
Information system boundary protections at a Guidance Any connections to the Internet, or other externations as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection strate concepts of managed interfaces described all of appropriate candidates for domain partition The organization carefully considers the intrining Commercial telecommunications services are	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessme ning. nsically shared nature of commercial telecommunications services in the implementation e commonly based on network components and consolidated management systems shar	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred to ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third
Information system boundary protections at a Guidance Any connections to the Internet, or other exter routers, firewalls, guards, encrypted tunnels) as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection strat concepts of managed interfaces described al of appropriate candidates for domain partition The organization carefully considers the intrin Commercial telecommunications services are party provided access lines and other service Therefore, when this situation occurs, the org	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessment ning.	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred to ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third urces of increased risk despite contract security provisions.
Information system boundary protections at a Guidance Any connections to the Internet, or other exter routers, firewalls, guards, encrypted tunnels) as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection strat concepts of managed interfaces described al of appropriate candidates for domain partition The organization carefully considers the intrin Commercial telecommunications services are party provided access lines and other service Therefore, when this situation occurs, the org virtual private networks.	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa- tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessment ning. nsically shared nature of commercial telecommunications services in the implementation e commonly based on network components and consolidated management systems shar e elements. Consequently, such interconnecting transmission services may represent sour	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred to ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third urces of increased risk despite contract security provisions. epts the additional risk. NIST SP 800-77 provides guidance on
Information system boundary protections at a Guidance Any connections to the Internet, or other exter routers, firewalls, guards, encrypted tunnels) as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection strat concepts of managed interfaces described al of appropriate candidates for domain partition The organization carefully considers the intri Commercial telecommunications services are party provided access lines and other service Therefore, when this situation occurs, the org virtual private networks. Applicability: All	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa- tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessment ning. nsically shared nature of commercial telecommunications services in the implementation e commonly based on network components and consolidated management systems shar ganization either implements appropriate compensating security controls or explicitly acce	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred to ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third urces of increased risk despite contract security provisions. epts the additional risk. NIST SP 800-77 provides guidance on
Information system boundary protections at a Guidance Any connections to the Internet, or other externations as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection stratt concepts of managed interfaces described al of appropriate candidates for domain partition The organization carefully considers the intrin Commercial telecommunications services are party provided access lines and other services Therefore, when this situation occurs, the org- virtual private networks. Applicability: All ASSESSMENT PROCEDURE: SC-7.1	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa- tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessment ning. nsically shared nature of commercial telecommunications services in the implementation e commonly based on network components and consolidated management systems shar ganization either implements appropriate compensating security controls or explicitly acce	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred to ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third urces of increased risk despite contract security provisions.
Information system boundary protections at a Guidance Any connections to the Internet, or other exter routers, firewalls, guards, encrypted tunnels) as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection strat concepts of managed interfaces described al of appropriate candidates for domain partition The organization carefully considers the intrin Commercial telecommunications services are party provided access lines and other service Therefore, when this situation occurs, the org	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa- tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessment ning. nsically shared nature of commercial telecommunications services in the implementation e commonly based on network components and consolidated management systems shar ganization either implements appropriate compensating security controls or explicitly acce	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred to ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third urces of increased risk despite contract security provisions. epts the additional risk. NIST SP 800-77 provides guidance on
Information system boundary protections at a Guidance Any connections to the Internet, or other externations as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection stratic concepts of managed interfaces described all of appropriate candidates for domain partition The organization carefully considers the intrinic Commercial telecommunications services are party provided access lines and other services Therefore, when this situation occurs, the org- virtual private networks. Applicability: All ASSESSMENT PROCEDURE: SC-7.1 Assessment Objective	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa- tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessment ning. nsically shared nature of commercial telecommunications services in the implementation e commonly based on network components and consolidated management systems shar e elements. Consequently, such interconnecting transmission services may represent sou ganization either implements appropriate compensating security controls or explicitly access References: ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred t ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third urces of increased risk despite contract security provisions. epts the additional risk. NIST SP 800-77 provides guidance on
Information system boundary protections at a Guidance Any connections to the Internet, or other externations as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection stratt concepts of managed interfaces described al of appropriate candidates for domain partition The organization carefully considers the intrin Commercial telecommunications services are party provided access lines and other services Therefore, when this situation occurs, the org- virtual private networks. Applicability: All ASSESSMENT PROCEDURE: SC-7.1 Assessment Objective Determine if: (i) the organization defines key internal bound	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa- tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessment ning. nsically shared nature of commercial telecommunications services in the implementation e commonly based on network components and consolidated management systems shar e elements. Consequently, such interconnecting transmission services may represent sou ganization either implements appropriate compensating security controls or explicitly access References: ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred t ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include thircu urces of increased risk despite contract security provisions. epts the additional risk. NIST SP 800-77 provides guidance on Related Controls: AC-4, CA-3, MP-4, RA-
Information system boundary protections at a Guidance Any connections to the Internet, or other externations as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection stratt concepts of managed interfaces described al of appropriate candidates for domain partition The organization carefully considers the intrin Commercial telecommunications services are party provided access lines and other services Therefore, when this situation occurs, the org- virtual private networks. Applicability: All ASSESSMENT PROCEDURE: SC-7.1 Assessment Objective Determine if: (i) the organization defines key internal bound	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa- tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessme ning. nsically shared nature of commercial telecommunications services in the implementation of e commonly based on network components and consolidated management systems shar e elements. Consequently, such interconnecting transmission services may represent sou ganization either implements appropriate compensating security controls or explicitly acce References: ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred to ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third urces of increased risk despite contract security provisions. epts the additional risk. NIST SP 800-77 provides guidance on Related Controls: AC-4, CA-3, MP-4, RA-
Information system boundary protections at a Guidance Any connections to the Internet, or other externations as a demilitarized zone or DMZ). Information As part of a defense-in-depth protection stratt concepts of managed interfaces described al of appropriate candidates for domain partition The organization carefully considers the intrin Commercial telecommunications services are party provided access lines and other services Therefore, when this situation occurs, the org- virtual private networks. Applicability: All ASSESSMENT PROCEDURE: SC-7.1 Assessment Objective Determine if: (i) the organization defines key internal boun- (ii) the information system monitors and cont Assessment Methods And Objects	any designated alternate processing site shall provide the same levels of protection as the ernal networks or information systems, occur through managed interfaces consisting of ap a arranged in an effective architecture (e.g., routers protecting firewalls and application gat a system boundary protections at any designated alternate processing sites provide the sa- tegy, the organization considers partitioning higher-impact information systems into separ bove to restrict or prohibit network access in accordance with an organizational assessme ning. nsically shared nature of commercial telecommunications services in the implementation of e commonly based on network components and consolidated management systems shar e elements. Consequently, such interconnecting transmission services may represent sou ganization either implements appropriate compensating security controls or explicitly acce References: ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	ease of information outside of the information system boundary. ose of the primary site. ppropriate boundary protection devices (e.g., proxies, gateways, teways residing on a protected subnetwork commonly referred t ame levels of protection as that of the primary site. rate physical domains (or environments) and applying the ent of risk. FIPS 199 security categorization guides the selection of security controls associated with the use of such services. red by all attached commercial customers, and may include third urces of increased risk despite contract security provisions. epts the additional risk. NIST SP 800-77 provides guidance on Related Controls: AC-4, CA-3, MP-4, RA-

	on hardware and software; information system configuration settings and associated documentation;	other relevant documents or records.
	al personnel with boundary protection responsibilities.	
	ing and control of communications at the external boundary of the information system and at key inter a capability within the information system.	rnal boundaries within the system; automated mechanisms
SC-7(1) – Enhancement (High)		
Control		
	sible information system components (e.g., public web servers, public email servers, public DNS serv	ers) to senarate sub-networks with senarate physical network
interfaces.		ers) to separate sub-networks with separate physical network
Guidance		
Publicly accessible information sy	stem components include, for example, public web servers.	
Applicability: All	References: ARS: SC-7(1); NIST 800-53/53A: SC-7(1)	Related Controls:
ASSESSMENT PROCEDURE: SC		
Assessment Objective		
-	sically allocates publicly accessible information system components to separate subnetworks with ser	parate, physical network interfaces.
Assessment Methods And Object	cts	
Examine: System and communic	ations protection policy; procedures addressing boundary protection; information system design docu	mentation; information system hardware and software;
information system architecture; ir	nformation system configuration settings and associated documentation; other relevant documents or	records.
SC-7(2) – Enhancement (High)		
Control		
Prevent public access into the inte	ernal networks except as appropriately mediated.	
Applicability: All	References: ARS: SC-7(2); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(2)	Related Controls:
ASSESSMENT PROCEDURE: SC	2-7(2).1	
Assessment Objective		
Determine if:		
	ediation necessary for public access to the organization's internal networks; and	
	ic access into the organization's internal networks except as appropriately mediated.	
Assessment Methods And Object		
	ations protection policy; procedures addressing boundary protection; list of mediation vehicles for allo	
	entation; boundary protection hardware and software; information system configuration settings and a plementing access controls for public access to the organization's internal networks.	associated documentation; other relevant documents or records
SC-7(3) – Enhancement (High)	Sementing access controls for public access to the organization's internal networks.	
Control	to the information exchanges to ellow for botton mentioning of inhoused and excland a structured to fin	
Applicability: All	to the information system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3)	Related Controls:
ASSESSMENT PROCEDURE: SC		Related Controls:
Assessment Objective	<u>~1(3).1</u>	
	s the number of access points to the information system to allow for better monitoring of inbound and	outbound network traffic
Assessment Methods And Object		
	ations protection policy; procedures addressing boundary protection; information system design docu	mentation: boundary protection bardware and software.
	nd configuration documentation; information system configuration settings and associated documentation	
SC-7(4) – Enhancement (High)		
Control		
	h any external telecommunication service, implementing controls appropriate to the required protectio	n of the confidentiality and integrity of the information being
Applicability: All	References: ARS: SC-7(4); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(4)	Related Controls:
transmitted.	References: ARS: SC-7(4); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(4)	

ASSESSMENT PROCEDURE: SC-7(4).1

Assessment Objective

Determine if:

(i) the organization defines the security controls (i.e., boundary protection devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service: and

(ii) the organization implements a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.

SC-7(5) – Enhancement (High)

Control

Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.

Applicability: All	References: ARS: SC-7(5); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(5)	Related Controls:
ASSESSMENT PROCEDURE: SC-7(5).1	-	

Assessment Objective

Determine if the information system denies network traffic by default and allows network traffic by exception.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation: other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.

SC-7(CMS-1) – Enhancement (High)

Control

Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Applicability: All	References: ARS: SC-7(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SC-7(CMS-1).1		

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation: boundary protection hardware and software: information system configuration settings and associated documentation: and other relevant documents or records to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; and automated mechanisms implementing boundary protection capability within the information system to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

SC-7(CMS-2) – Enhancement (High)

Control

Utilize stateful inspection / application firewall hardware and software. References: ARS: SC-7(CMS-2): FISCAM: TAC-3.2.E.1 Applicability: All

Related Controls:

ASSESSMENT PROCEDURE: SC-7(CMS-2).1 Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; and automated mechanisms implementing boundary protection capability within the information system to determine if the organization utilizes stateful inspection / application firewall hardware and software.

SC-7(CMS-3) – Enhancement (High)

Control

Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Applicability: All	References: ARS: SC-7(CMS-3)	Related Controls:
ASSESSMENT PROCEDURE: SC-7(CMS-3).		

Assessment Objective

Determine if the organization defines key internal boundaries of the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system to determine if the organization utilizes firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

SC-8 – Transmission Integrity (High)

Control

Procedures shall be developed and documented, and technical controls shall be established and implemented effectively to protect the integrity of CMS information while in transit.

Guidance

If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission integrity using IPSec. NIST SP 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Applicability: All	References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PISP: 4.16.8	Related Controls:

ASSESSMENT PROCEDURE: SC-8.1

Assessment Objective

Determine if the information system protects the integrity of transmitted information.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Transmission integrity capability within the information system.

SC-8(1) – Enhancement (High)

Control

Employ approved cryptographic mechanisms to ensure recognition of changes to information during transmission.

Guidance

Alternative physical protection measures include, for example, protected distribution systems.

Applicability: All	References: ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(c)(1); NIST 800- 53/53A: SC-8(1)	Related Controls:
ASSESSMENT PROCEDURE: SC-8(1).1		
Assessment Objective Determine if the information system employs cry	ptographic mechanisms to recognize changes to information during transmission unless otherwise prote	cted by alternative physical measures
associated documentation; other relevant docum		nation system configuration settings and
	transmission integrity capability within the information system.	
SC-8(CMS-1) – Enhancement (High)		
Control Employ appropriate approved mechanisms (e.g. SC-13, Use of Cryptography, PISP 4.16.13).	, digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to de	estination outside of a secured network (see
Applicability: All	References: ARS: SC-8(CMS-1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(c)(1), 164.312(e)(2)(i)	Related Controls: SC-13
ASSESSMENT PROCEDURE: SC-8(CMS-1).1		
Assessment Objective Determine if the information system protects the Assessment Methods And Objects	integrity of transmitted information.	
associated documentation; and other relevant do protect the integrity of data while in transit from s Interview: Network administrators to determine transit from source to destination outside of a se Test: Transmission integrity capability within the protect the integrity of data while in transit from s	on policy; procedures addressing transmission integrity; information system design documentation; inform ocuments or records to determine if the organization employs appropriate approved mechanisms (e.g., or source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13). if the organization employs appropriate approved mechanisms (e.g., digital signatures, cryptographic has curred network (see SC-13, Use of Cryptography, PISP 4.16.13). information system to determine if the organization employs appropriate approved mechanisms (e.g., di source to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13).	ligital signatures, cryptographic hashes) to shes) to protect the integrity of data while in
SC-9 – Transmission Confidentiality (H	igh)	
Control		
	d, and technical controls shall be established and implemented effectively to protect the confidentiality of	CMS sensitive information while in transit.
assurances regarding the implementation of nee control effectiveness through appropriate contra	rvice provider for transmission services as a commodity item rather than a fully dedicated service, it may aded security controls for transmission confidentiality. When it is infeasible or impractical to obtain the nec cting vehicles, the organization either implements appropriate compensating security controls or explicitly onfidentiality using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting tran ctive Distribution Systems.	cessary security controls and assurances of accepts the additional risk. NIST SP 800-52
Applicability: All	References: ARS: SC-9; HIPAA: 164.312(e)(1); IRS-1075: 5.6.3.4#2, 5.6.3.4#4.1; NIST 800-53/53A: SC-9; PISP: 4.16.9	Related Controls: AC-17
ASSESSMENT PROCEDURE: SC-9.1	•	
information system configuration settings and as	on policy; procedures addressing transmission confidentiality; information system design documentation; sociated documentation; other relevant documents or records.	contracts for telecommunications services;
Test: Transmission confidentiality capability with	nin the information system.	
SC-9(1) – Enhancement (High)		
Control Encryption is not required within a secured netw	ork. When transmitting data outside of a secured network:	
D		

Guidance	cuits must be used.	
	de, for example, protected distribution systems.	
Applicability: All	References: ARS: SC-9(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(e)(1), 164.312(e)(2)(ii IRS-1075: 5.6.3.4#2, 5.7#1; NIST 800-53/53A: SC-9(1)); Related Controls: SC-13
ASSESSMENT PROCEDURE: SC-9(1).1		- ·
Assessment Objective		
Determine if the information system employs on measure.	ryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless	otherwise protected by alternative physical
Assessment Methods And Objects		
hardware and software or Protected Distribution	tion policy; procedures addressing transmission confidentiality; information system design documentation on System protection mechanisms; information system configuration settings and associated documentation of the section of the table of the section of the se	
	g transmission confidentiality capability within the information system.	
SC-9(PII-1) – Enhancement (High) Control		
fax machines must be located in a secured are explicitly provides guidance to the recipient tha necessary) to report the disclosure and confirm		and (iii) a cover sheet must be used that ded recipients to telephone the sender (collect i
Applicability: All ASSESSMENT PROCEDURE: SC-9(PII-1).1	References: IRS-1075: 5.7.4#1	Related Controls:
Assessment Objective		
must be used that explicitly provides guidance	be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recip to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and lisclosure and confirm destruction of the information.	
-	stodial coverage of outgoing and incoming PII transmitted data.	
Test: Send or receive a simulated PII fax to er		
frequent fax recipients is maintained; and (iii) a	erage over outgoing and incoming transmissions or fax machines is located in a secured area; (ii) accura a cover sheet is used that explicitly provides guidance to the recipient that includes: a notification of the s	
	is to telephone the sender (collect it necessary) to report the disclosure and contirm destruction of the in	formation
	ts to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the in	formation.
SC-10 – Network Disconnect (High)	ts to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the in	formation.
SC-10 – Network Disconnect (High) Control Technical controls shall be established and im	plemented effectively to ensure that network connections are properly terminated at the end of user sess	formation.
SC-10 – Network Disconnect (High) Control Technical controls shall be established and im conditions (e.g., a period of inactivity).		formation.
 SC-10 – Network Disconnect (High) Control Technical controls shall be established and im conditions (e.g., a period of inactivity). Guidance The organization applies this control within the 	plemented effectively to ensure that network connections are properly terminated at the end of user sess context of risk management that considers specific mission or operational requirements.	formation. sions, or upon the occurrence of specified
 SC-10 – Network Disconnect (High) Control Technical controls shall be established and im conditions (e.g., a period of inactivity). Guidance The organization applies this control within the Applicability: All 	plemented effectively to ensure that network connections are properly terminated at the end of user sess	formation.
SC-10 – Network Disconnect (High) Control Technical controls shall be established and im conditions (e.g., a period of inactivity). Guidance The organization applies this control within the Applicability: All ASSESSMENT PROCEDURE: SC-10.1	plemented effectively to ensure that network connections are properly terminated at the end of user sess context of risk management that considers specific mission or operational requirements.	formation. sions, or upon the occurrence of specified
SC-10 – Network Disconnect (High) Control Technical controls shall be established and im conditions (e.g., a period of inactivity). Guidance The organization applies this control within the Applicability: All ASSESSMENT PROCEDURE: SC-10.1 Assessment Objective Determine if: (i) the organization defines the time period of in (ii) the information system terminates a networ	plemented effectively to ensure that network connections are properly terminated at the end of user sess context of risk management that considers specific mission or operational requirements.	formation. sions, or upon the occurrence of specified
SC-10 – Network Disconnect (High) Control Technical controls shall be established and im conditions (e.g., a period of inactivity). Guidance The organization applies this control within the Applicability: All ASSESSMENT PROCEDURE: SC-10.1 Assessment Objective Determine if: (i) the organization defines the time period of in (ii) the information system terminates a networ Assessment Methods And Objects	plemented effectively to ensure that network connections are properly terminated at the end of user sess context of risk management that considers specific mission or operational requirements. References: ARS: SC-10; NIST 800-53/53A: SC-10; PISP: 4.16.10 hactivity before the information system terminates a network connection; and k connection at the end of a session or after the organization-defined time period of inactivity.	formation. sions, or upon the occurrence of specified Related Controls:
SC-10 – Network Disconnect (High) Control Technical controls shall be established and im conditions (e.g., a period of inactivity). Guidance The organization applies this control within the Applicability: All ASSESSMENT PROCEDURE: SC-10.1 Assessment Objective Determine if: (i) the organization defines the time period of in (ii) the information system terminates a networ Assessment Methods And Objects Examine: System and communications protect	plemented effectively to ensure that network connections are properly terminated at the end of user sess context of risk management that considers specific mission or operational requirements. References: ARS: SC-10; NIST 800-53/53A: SC-10; PISP: 4.16.10 hactivity before the information system terminates a network connection; and	formation. sions, or upon the occurrence of specified Related Controls:

Test: Network disconnect capability within the information system.
SC-10(0) – Enhancement (High)
Control
Configure the information system to forcibly disconnect network connections at the end of a session, or after fifteen (15) minutes of inactivity, for mainframe sessions.
Applicability: AllReferences: ARS: SC-10(0); FISCAM: TAC-3.2.C.3; NIST 800-53/53A: SC-10; PISP: 4.16.10Related Controls:
ASSESSMENT PROCEDURE: SC-10(0).1
Assessment Objective
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.
Assessment Methods And Objects
Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before
network disconnect; information system configuration settings and associated documentation; other relevant documents or records.
Test: Network disconnect capability within the information system.
SC-11 – Trusted Path (High)
Control
Technical controls shall be established and implemented effectively to provide the capability to establish trusted communications paths between authorized users and the security functionality of the information system.
Guidance
A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).
Applicability: All References: ARS: SC-11; NIST 800-53/53A: SC-11; PISP: 4.16.11 Related Controls:
ASSESSMENT PROCEDURE: SC-11.1
Assessment Objective
Determine if:
(i) the organization defines the security functions within the information system that are included in a trusted communications path;
(ii) the organization-defined security functions include information system authentication and reauthentication; and
(iii) the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system.
Assessment Methods And Objects
Examine: System and communications protection policy; procedures addressing trusted communications paths; information system security plan; information system design documentation;
information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records. (Optional)
Test: Automated mechanisms implementing trusted communications paths within the information system.(Optional)
SC-11(0) – Enhancement (High)
Control
At a minimum, a trusted communications path is established between the user and the following system security functions: system authentication, re-authentication, and key management.
Applicability: All References: ARS: SC-11(0); FISCAM: TAC-3.2.E.1; PISP: 4.16.11 Related Controls:
ASSESSMENT PROCEDURE: SC-11(0).1
Assessment Objective
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.
Assessment Methods And Objects
Examine: System and communications protection policy; procedures addressing trusted communications paths; information system security plan (for organization-defined security functions to
include for authentication and reauthentication); information system design documentation; information system configuration settings and associated documentation; assessment results from
independent, testing organizations; other relevant documents or records.
Test: Automated mechanisms implementing trusted communications paths within the information system.
SC-12 – Cryptographic Key Establishment and Management (High)
Control
When cryptography is required and used within the information system, documented procedures shall be implemented effectively for cryptographic key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect sensitive information shall be controlled and distributed using the NIST SP 800-56 and NIST SP 800-57 approved key management
quidance.

Guidance		
	ce on cryptographic key establishment. NIST SP 800-57 provides guidance on cryptographic key management. References: ARS: SC-12; IRS-1075: 5.7.1#1; NIST 800-53/53A: SC-12; PISP: 4.16.12	Related Controls:
Applicability: All ASSESSMENT PROCEDURE: SO		Related Controls:
Assessment Objective	-12.1	
•	ablishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual	procedures, when cryptography is required and
employed within the information s		procedures, when cryptography is required and
Assessment Methods And Obje	,	
Examine: System and communic	ations protection policy; procedures addressing cryptographic key management and establishment; NIST SP 80	00-56 and 800-57; information system design
	m configuration settings and associated documentation; other relevant documents or records.	
•	nel with responsibilities for cryptographic key establishment or management.	
	plementing cryptographic key management and establishment within the information system.	
SC-12(CMS-1) – Enhancement (I	High)	
Control	······································	
	with supporting procedures or manual procedures for cryptographic key establishment and key management. T coverable by authorized personnel, require senior management approval to authorize recovery of keys by other	
	13, Use of Cryptography, PISP 4.16.13).	than the key owner, and comply with approved
Applicability: All	References: ARS: SC-12(CMS-1)	Related Controls: MA-CMS-1, MA-CMS-2
		SC-13
ASSESSMENT PROCEDURE: SO	C-12(CMS-1).1	
Assessment Objective		
	ablishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual	procedures, when cryptography is required and
employed within the information s	•	
Assessment Methods And Obje		
	cations protection policy; procedures addressing cryptographic key management and establishment; NIST SP 80 m configuration settings and associated documentation; and other relevant documents or records to determine i	
	inual procedures for cryptographic key establishment and key management. The mechanisms and procedures	
(see SC-13, Use of Cryptography		
	ional personnel with responsibilities for cryptographic key establishment or management to determine if the orga	
	procedures for cryptographic key establishment and key management. The mechanisms and procedures shall	comply with approved cryptography standards (see
SC-13, Use of Cryptography, PIS	P 4.16.13). plementing cryptographic key management and establishment within the information system to determine if the	organization amploys outomated machanisms with
	procedures for cryptographic key establishment and establishment within the mornation system to determine if the	
SC-13, Use of Cryptography, PIS		
SC-13 – Use of Cryptography		
Control		
	are used, procedures shall be developed, documented, and implemented effectively to ensure they comply with	h applicable laws, Executive Orders, directives,
	nd guidance. All such mechanisms shall be FIPS 140-2 (as amended and revised) compliant and NIST validate	
Guidance		
	or employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation	
	PS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued	
cryptography is available at http://	0-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Add	unional information on the use of validated
	(csrc nist dov/cryptyal	
Applicability: All		3.4#2. Related Controls: AC-17(CMS-1) AC-
Applicability: All	/csrc.nist.gov/cryptval. References: ARS: SC-13; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3 5.6.3.4#4.2-3; NIST 800-53/53A: SC-13; PISP: 4.16.13	19(CMS-1), AC-3, AC-3(CMS-1), MP-
Applicability: All	References: ARS: SC-13; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3	

ASSESSMENT PROCEDURE: SC-13.1		
Assessment Objective		
Determine if for information requiring cryptograp	phic protection, the information system implements cryptographic mechanisms tha	t comply with applicable laws, Executive Orders, directives, policies
regulations, standards, and guidance.		
Assessment Methods And Objects		
	ion policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); on settings and associated documentation; cryptographic module validation certifica	
SC-14 – Public Access Protections (Hi	gh)	
Control		
Technical controls shall be developed, docume	nted, and implemented effectively to protect the integrity of the publicly accessible	CMS information and applications.
Guidance		
CMS refers to the National Institute of Standard	s and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix A	provides a summary for remote access controls.
pplicability: All	References: ARS: SC-14; NIST 800-53/53A: SC-14; PISP: 4.16.14	Related Controls:
SSESSMENT PROCEDURE: SC-14.1		
ssessment Objective		
	e integrity and availability of publicly available information and applications.	
Assessment Methods And Objects		
•	ion policy; procedures addressing public access protections; access control policy	and procedures: boundary protection procedures: information
	em configuration settings and associated documentation; other relevant document	
	ccess controls and boundary protection for publicly available information and applic	
C-14(CMS-1) – Enhancement (High)		
Control	outer file norminations, and application configurations protect the integrity of info	rmation stared processed and transmitted by publicly accessible
systems, as well as the integrity of publicly access	system file permissions, and application configurations protect the integrity of info	mation stored, processed, and transmitted by publicly accessible
Applicability: All	References: ARS: SC-14(CMS-1); FISCAM: TAC-3.2.E.1	Related Controls:
SSESSMENT PROCEDURE: SC-14(CMS-1)		Related Controls.
ssessment Objective		
-	e integrity and availability of publicly available information and applications.	
ssessment Methods And Objects	a integrity and availability of publicity available information and applications.	
	ion naliou procedures addressing public second protections, second control policy	and presedures, houndary protection presedures, information
	ion policy; procedures addressing public access protections; access control policy em configuration settings and associated documentation; and other relevant docur	
	urations protect the integrity of information stored, processed, and transmitted by p	
accessible applications.	and the integrity of information stored, processed, and transmitted by p	denois accessible systems, as well as the integrity of publicity
	ne if network access controls, operating system file permissions, and application c	
Interview: Organizational personnel to determine		configurations protect the integrity of information stored, processed.
		onfigurations protect the integrity of information stored, processed,
and transmitted by publicly accessible systems	, as well as the integrity of publicly accessible applications.	
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to		
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessit	, as well as the integrity of publicly accessible applications. o determine if network access controls, operating system file permissions, and app	
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessible C-14(CMS-2) – Enhancement (High)	, as well as the integrity of publicly accessible applications. o determine if network access controls, operating system file permissions, and app	
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessib SC-14(CMS-2) – Enhancement (High) Control	, as well as the integrity of publicly accessible applications. o determine if network access controls, operating system file permissions, and app ble systems, as well as the integrity of publicly accessible applications.	lication configurations protect the integrity of information stored,
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessib SC-14(CMS-2) – Enhancement (High) Control If e-authentication is required and implemented	, as well as the integrity of publicly accessible applications. o determine if network access controls, operating system file permissions, and app ble systems, as well as the integrity of publicly accessible applications.	lication configurations protect the integrity of information stored, A for e-Authentication Standards.
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessib C-14(CMS-2) – Enhancement (High) Control If e-authentication is required and implemented pplicability: All	, as well as the integrity of publicly accessible applications. o determine if network access controls, operating system file permissions, and app ble systems, as well as the integrity of publicly accessible applications.	lication configurations protect the integrity of information stored,
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessib C-14(CMS-2) – Enhancement (High) Control If e-authentication is required and implemented applicability: All ASSESSMENT PROCEDURE: SC-14(CMS-2)	, as well as the integrity of publicly accessible applications. o determine if network access controls, operating system file permissions, and app ble systems, as well as the integrity of publicly accessible applications.	lication configurations protect the integrity of information stored, A for e-Authentication Standards.
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessib C-14(CMS-2) – Enhancement (High) Control If e-authentication is required and implemented applicability: All SSESSMENT PROCEDURE: SC-14(CMS-2) Assessment Objective	, as well as the integrity of publicly accessible applications. b determine if network access controls, operating system file permissions, and app ble systems, as well as the integrity of publicly accessible applications. I in conjunction with or related to public access protections, refer to ARS Appendix References: ARS: SC-14(CMS-2)).1	lication configurations protect the integrity of information stored, A for e-Authentication Standards.
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessib C-14(CMS-2) – Enhancement (High) Control If e-authentication is required and implemented applicability: All ASSESSMENT PROCEDURE: SC-14(CMS-2) Assessment Objective Determine if the information system protects the	, as well as the integrity of publicly accessible applications. o determine if network access controls, operating system file permissions, and app ble systems, as well as the integrity of publicly accessible applications.	lication configurations protect the integrity of information stored, A for e-Authentication Standards.
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessible C-14(CMS-2) – Enhancement (High) Control If e-authentication is required and implemented pplicability: All SSESSMENT PROCEDURE: SC-14(CMS-2) ISSESSMENT Objective Determine if the information system protects the SSESSMENT Methods And Objects	, as well as the integrity of publicly accessible applications. b determine if network access controls, operating system file permissions, and app ble systems, as well as the integrity of publicly accessible applications. I in conjunction with or related to public access protections, refer to ARS Appendix References: ARS: SC-14(CMS-2)).1 e integrity and availability of publicly available information and applications.	A for e-Authentication Standards. Related Controls:
and transmitted by publicly accessible systems, Test: Interfaces for all public-facing networks to processed, and transmitted by publicly accessible C-14(CMS-2) – Enhancement (High) Control If e-authentication is required and implemented pplicability: All SSESSMENT PROCEDURE: SC-14(CMS-2) ISSESSMENT Objective Determine if the information system protects the SSESSMENT Methods And Objects	, as well as the integrity of publicly accessible applications. b determine if network access controls, operating system file permissions, and app ble systems, as well as the integrity of publicly accessible applications. I in conjunction with or related to public access protections, refer to ARS Appendix References: ARS: SC-14(CMS-2)).1	A for e-Authentication Standards. Related Controls:

system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.

Interview: MA owners for each public-facing MA to determine if e-authentication is required and implemented in conjunction with or related to public access protections; refer to ARS Appendix A for e-Authentication Standards.

Test: All public-facing systems to determine if e-authentication is required and implemented in conjunction with or related to public access protections; refer to ARS Appendix A for e-Authentication Standards.

SC-15 – Collaborative Computing (High)

Control

Running collaborative computing mechanisms on CMS information systems shall require authorization by the CIO or his/her designated representative. The authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used. Collaborative computing mechanisms shall not be activated remotely.

Guidance

Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

Applicability: All	References: ARS: SC-15; NIST 800-53/53A: SC-15; PISP: 4.16.15	Related Controls:
ASSESSMENT PROCEDURE: SC-15.1		

Assessment Objective

Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users.

SC-15(1) – Enhancement (High)

Control

If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:

Provide physical disconnect of cameras or microphones in a manner that supports ease of use.

Applicability: All	References: ARS: SC-15(1); NIST 800-53/53A: SC-15(1)	Related Controls:
ASSESSMENT PROCEDURE: SC-15(1).1		

Assessment Objective

Determine if the information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Physical disconnect of collaborative computing devices.(Optional)

SC-15(CMS-1) – Enhancement (High)

Control

If collaborative computing mechanisms are authorized in writing by the CIO or his/her designated representative:

Ensure the information system provides:

(a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and

(b) Explicit indication to the local user of the fact that it is in use.

 Applicability: All
 References: ARS: SC-15(CMS-1)
 Related Controls:

 ASSESSMENT PROCEDURE: SC-15(CMS-1).1
 Controls:
 Controls:

Assessment Objective

Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the information system provides: (a) An explicit description of acceptable use of collaborative computing mechanisms to the local users (e.g., camera or microphone), and

 (b) Explicit indication to the local user of the farest: Automated mechanisms implementing a (a) An explicit description of acceptable use of (b) Explicit indication to the local user of the farest SC-16 – Transmission of Security Para Control 	nation system provides: collaborative computing mechanisms to the local users (e.g., camera or microphone), and ct that it is in use. ccess controls for collaborative computing environments and alert notification for local users to determine collaborative computing mechanisms to the local users (e.g., camera or microphone), and ct that it is in use.	
Guidance	with labels and markings. Security perspectate may be explicitly at implicitly appreciated with the information	a contained within the information evotors
Applicability: All	urity labels and markings. Security parameters may be explicitly or implicitly associated with the informatic References: ARS: SC-16: NIST 800-53/53A: SC-16: PISP: 4.16.16	Related Controls:
ASSESSMENT PROCEDURE: SC-16.1	References. ANS. 50-10, NIST 600-55/55A. 50-10, FISF. 4.10.10	Related Controls.
Assessment Objective	sociates security parameters with information exchanged between information systems.	
Assessment Methods And Objects	sociales security parameters with mormation exchanged between mormation systems.	
Examine: System and communications protect information system design documentation; information; inform; information; information; inform; inform; inf	tion policy; procedures addressing transmission of security parameters; access control policy and procedure trmation system configuration settings and associated documentation; other relevant documents or record ble transmission of security parameters between information systems.(Optional)	ures; boundary protection procedures; ls.(Optional)
SC-17 – Public Key Infrastructure Cert	ificates (High)	
key certificate shall include authorization by a certificate is issued to the intended party.	information system shall be issued in accordance with a defined certification policy and certification practi supervisor or a responsible official, and shall be done by a secure process that verifies the identity of the o	
	lishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at me required by OMB Memorandum 05-24. NIST SP 800-32 provides guidance on public key technology. NIS	
Applicability: All	References: ARS: SC-17; NIST 800-53/53A: SC-17; PISP: 4.16.17	Related Controls:
ASSESSMENT PROCEDURE: SC-17.1		
provider. Assessment Methods And Objects Examine: System and communications protect 32; other relevant documents or records.	v certificates under an appropriate certificate policy or obtains public key certificates under an appropriate etion policy; procedures addressing public key infrastructure certificates; public key certificate policy or poli	
SC-18 – Mobile Code (High)	c key minastructure certaincate issuing responsibilities.	
Control CMS shall establish usage restrictions and im document, monitor, and implement controls fo implement controls and procedures for mobile	plementation guidance for mobile code technologies based on the potential to cause harm to CMS informat r the use of mobile code within the CMS information system. Appropriate officials shall authorize or deny to code in accordance with NIST SP 800-28.	ation systems. The organization shall the use of mobile code. The organization shall
0 1	e, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage code installed on organizational servers and mobile code downloaded and executed on individual workstat	0

Applicability: All	References: ARS: SC-18; NIST 800-53/53A: SC-18; PISP: 4.16.18	Related Controls:
ASSESSMENT PROCEDURE: SC-18.1		
Assessment Objective		
Determine if:		
(i) the organization establishes usage restriction	ns and implementation guidance for mobile code technologies based on the potential to c	cause damage to the information system if used maliciously;
and		
(ii) the organization authorizes, monitors, and c	ontrols the use of mobile code within the information system.	
Assessment Methods And Objects		
, , , , , , , , , , , , , , , , , , , ,	ion policy; procedures addressing mobile code; mobile code usage restrictions, mobile co	ode implementation guidance; NIST SP 800-28; other releva
documents or records.		
	e code authorization, monitoring, and control responsibilities.	
Test: Mobile code authorization and monitoring		
SC-19 – Voice Over Internet Protocol (I	Hign)	
Control		
	lementation guidance for Voice over Internet Protocol (VoIP) technologies based on the p	
Guidance	Is for the use of VoIP within a CMS information system. When VoIP is implemented, the	organization shall adhere to the NIST SP 800-58 guidance.
Applicability: All	considerations for VoIP technologies employed in information systems. References: ARS: SC-19; NIST 800-53/53A; SC-19; PISP: 4.16.19	Related Controls:
Applicability. All	References. ARS. SC-19, NIST 600-55/55A. SC-19, FISF. 4.10.19	Related Controls.
ASSESSMENT DROCEDURE, SC 10.1		
Assessment Objective		
Assessment Objective Determine if:		
Assessment Objective Determine if: (i) the organization establishes usage restriction	ns and implementation guidance for Voice over Internet Protocol technologies based on t	the potential to cause damage to the information system if us
Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and		the potential to cause damage to the information system if us
(i) the organization establishes usage restriction maliciously; and(ii) the organization authorizes, monitors, and c	ns and implementation guidance for Voice over Internet Protocol technologies based on t ontrols the use of VoIP within the information system.	the potential to cause damage to the information system if us
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects	ontrols the use of VoIP within the information system.	
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect	ontrols the use of VoIP within the information system.	
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP	ontrols the use of VoIP within the information system.	
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High)	ontrols the use of VoIP within the information system.	
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities.	
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing b	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities.	relevant documents or records.
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing b Applicability: All	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1)	
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and con- Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing be Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1)	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1)	relevant documents or records.
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and co Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing b Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1) Assessment Objective	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1)	relevant documents or records.
Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and (ii) the organization authorizes, monitors, and co Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing b Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1) Assessment Objective Determine if:	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1)).1	relevant documents or records. Related Controls:
Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and (ii) the organization authorizes, monitors, and con- Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing b Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1) Assessment Objective Determine if:	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1)	relevant documents or records. Related Controls:
Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and (ii) the organization authorizes, monitors, and conserved Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing b Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1) Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1)).1	relevant documents or records. Related Controls:
Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and (ii) the organization authorizes, monitors, and co Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing be Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1) Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1)).1 Ins and implementation guidance for Voice over Internet Protocol technologies based on t	relevant documents or records. Related Controls:
Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and (ii) the organization authorizes, monitors, and con- Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing be Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1) Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and (ii) the organization authorizes, monitors, and con- Assessment Methods And Objects	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1)).1 hs and implementation guidance for Voice over Internet Protocol technologies based on t ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; and o	relevant documents or records. Related Controls: the potential to cause damage to the information system if us
Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing b Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1) Assessment Objective Determine if: (i) the organization establishes usage restriction maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect VoIP is authorized in writing by the CMS CIO, c Interview: Organizational personnel with VoIP	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1) .1 hs and implementation guidance for Voice over Internet Protocol technologies based on t ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; and o or his/her designated representative. authorization and monitoring responsibilities to determine if the information system provide	relevant documents or records. Related Controls: the potential to cause damage to the information system if us ther relevant documents or records to determine if the use or
Assessment Objective Determine if: (i) the organization establishes usage restrictior maliciously; and (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect Interview: Organizational personnel with VoIP SC-19(CMS-1) – Enhancement (High) Control The use of VoIP must be authorized in writing b Applicability: All ASSESSMENT PROCEDURE: SC-19(CMS-1) Assessment Objective Determine if: (i) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect (ii) the organization authorizes, monitors, and c Assessment Methods And Objects Examine: System and communications protect VoIP is authorized in writing by the CMS CIO, c Interview: Organizational personnel with VoIP	ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; other authorization and monitoring responsibilities. by the CMS CIO, or his/her designated representative. References: ARS: SC-19(CMS-1) .1 hs and implementation guidance for Voice over Internet Protocol technologies based on t ontrols the use of VoIP within the information system. ion policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictions; and o or his/her designated representative. authorization and monitoring responsibilities to determine if the information system provide collaborative computing mechanisms to the local users (e.g., camera or microphone), and	relevant documents or records. Related Controls: the potential to cause damage to the information system if us ther relevant documents or records to determine if the use o

SC-20 – Secure Name / Address Resolution Service (Authoritative Source) (High) Control Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries. Guidance This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment. Applicability: All References: ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20 Assessment Objective Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries. Assessment Methods And Objectis Assessment Methods And Objects				
Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries. Guidance This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment. Applicability: All References: ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20 Related Controls: ASSESSMENT PROCEDURE: SC-20.1 Assessment Objective Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				
Guidance This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment. Applicability: All References: ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20 Related Controls: Assessment Objective Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				
This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment. Applicability: All References: ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20 Related Controls: Assessment Objective Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				
resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment. Applicability: All References: ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20 Related Controls: ASSESSMENT PROCEDURE: SC-20.1 Assessment Objective Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries. Internet provides artifacts for additional data integrity artifacts along with the authoritative data it returns in response to resolution queries.				
Applicability: All References: ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20 Related Controls: ASSESSMENT PROCEDURE: SC-20.1 Assessment Objective Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				
ASSESSMENT PROCEDURE: SC-20.1 Assessment Objective Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				
Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				
Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				
Assessment Methods And Objects				
Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); NIST SP 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.				
Test: Automated mechanisms implementing secure name/address resolution service (authoritative source) within the information system.				
SC-20(1) – Enhancement (High)				
Control				
When the information system is operating as part of a distributed, hierarchical namespace, ensure that it provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.				
Guidance				
An example means to indicate the security status of child subspaces is through the use of delegation signer resource records.				
Applicability: All References: ARS: SC-20(1); NIST 800-53/53A: SC-20(1) Related Controls:				
ASSESSMENT PROCEDURE: SC-20(1).1				
Assessment Objective				
Determine if the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.				
Assessment Methods And Objects				
Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)				
Test: Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services within the information system. (Optional)				
SC-21 – Secure Name / Address Resolution Service (Recursive or Caching Resolver) (High)				
Control				
Technical controls shall be developed, documented, and implemented effectively to ensure that each information system that provides name / address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.				
Guidance				
A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST SP 800-81 provides guidance on secure domain name system deployment.				
Applicability: All References: ARS: SC-21; NIST 800-53/53A: SC-21; PISP: 4.16.21 Related Controls:				
ASSESSMENT PROCEDURE: SC-21.1				
Assessment Objective				
Determine if the information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.				
Assessment Methods And Objects				
Examine: System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation;				
information system configuration settings and associated documentation; other relevant documents or records. Rev. 9 Page 183 of 207 BPSSM Appendix A, Attachment 1				

Test: Automated mechanisms implementing data origin authentication and integrity verification for resolution services within the information system.				
SC-22 – Architecture and Provisioning for Name / Address Resolution Service (High)				
Control				
Information systems that collectively provide name / address resolution service for an organization shall be fault tolerant and implement role separation.				
Guidance				
A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two s network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divid networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is guidance on secure DNS deployment.	ervers are commonly located in two different ed into those resources belonging to internal server with the internal role provides only provides name/address resolution also specified. NIST SP 800-81 provides			
Applicability: All References: ARS: SC-22; NIST 800-53/53A: SC-22; PISP: 4.16.22	Related Controls:			
ASSESSMENT PROCEDURE: SC-22.1 Assessment Objective				
Determine if the information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation. Assessment Methods And Objects Examine: System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; NIST SP 800-81; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents.				
Test: Automated mechanisms supporting name/address resolution service for fault tolerance and role separation.				
SC-23 – Session Authenticity (High)				
Control Technical controls shall be developed, documented, and effectively implemented to ensure that CMS information systems provide mechanisms to protect Guidance This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection architectures providing web-based services). NIST SP 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST SP 800- IPSec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST SP 800-95 provides guidance on secure web ser	where needed (e.g., in service-oriented 77 provides guidance on the deployment of			
Applicability: All References: ARS: SC-23; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-23; PISP: 4.16.23	Related Controls:			
ASSESSMENT PROCEDURE: SC-23.1				
Assessment Objective Determine if the information system provides mechanisms to protect the authenticity of communications sessions. Assessment Methods And Objects Examine: System and communications protection policy; procedures addressing session authenticity; NIST SP 800-52, 800-77, and 800-95; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing session authenticity.				
SC-CMS-1 – Desktop Modems (High)				
Control				
Users are prohibited from installing desktop modems.				
Guidance				
Desktop Modems allow backdoors into the network putting the CMS data and network at very high risk.				
Applicability: All References: ARS: SC-CMS-1; PISP: 4.16.24	Related Controls:			
ASSESSMENT PROCEDURE: SC-CMS-1.1				
Assessment Objective Determine if the organization has implement a policy which assists in prohibiting the installation of unauthorized desktop modems.				

Assessment Methods And Objects	
Examine: Organizational policy does not allow unauthorized desktop modems.	
SC-CMS-2 – Identify and Detect Unauthorized Modems (High)	
Control	
Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unaut	thorized modems.
Guidance	
It is good practice that management approve any automated tool or utility for checking for unauthorized modems.	
Applicability: All References: ARS: SC-CMS-2; PISP: 4.16.25	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-2.1	
Assessment Objective	
Determine if the organization has an approved automated system to test for unauthorized modems.	
Assessment Methods And Objects	
Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network ser	vices (e.g. modems, etc.) are available on demand and the
organization performs a complete review no less than quarterly.	
Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network set	ervices (e.g., modems, etc.) are available on demand and the
organization performs a complete review no less than quarterly.	
SC-CMS-2(CMS-0) – Enhancement (High)	
Control	
Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Per	form a complete review no less than quarterly.
Applicability: All References: ARS: SC-CMS-2(CMS-0)	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1	
Assessment Objective	
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescri	ibad in this amplifying aphancoment to the baseline central
Assessment Methods And Objects	ibed in this amplifying enhancement to the baseline control.
Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network ser	visos (o.g., modoms, oto) are available on domand and the
organization performs a complete review no less than guarterly.	vices (e.g., moderns, etc.) are available on demand and the
Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network systems	ervices (e.g., modems, etc.) are available on demand and the
organization performs a complete review no less than quarterly.	
Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., moder	ms, etc.) are available. Perform a complete review no less than
quarterly.	, , , , , , , , , , , , , , , , , , , ,
SC-CMS-3 – Secondary Authentication and Encryption (High)	
Control	
Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect	the in-transit confidentiality of their sessions outside the secure
network.	······································
Guidance	
A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP.	
Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-3.1	
Assessment Objective	
Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit.	
Assessment Methods And Objects	
Examine: In-transit technical controls implement and documents for sensitive information outside the secure network.	
SC-CMS-3(CMS-0) – Enhancement (High)	
Control	
Enable and force use of application security mechanisms, such as Transport Layer Security (TLS). Utilize CMS-approved encryption a	ind password authentication methods, in combination with
certificate-based authentication or additional authentication protection (e.g., token-based, biometric).	איז

Applicability: All	References: ARS: SC-CMS-3(CMS-0)	Related Controls:
ASSESSMENT PROCEDURE: S	SC-CMS-3(CMS-0).1	
Assessment Objective		
Determine if the organization m	eets the requirements as specified in the baseline control and the specific CMS	requirements as prescribed in this amplifying enhancement to the baseline control.
Assessment Methods And Obj	ects	
	termine if the organization enables and forces use of application security mecha ds, in combination with certificate-based authentication or additional authenticati	
Interview: Organizational perso	onnel to determine if the organization enables and forces use of application secu	urity mechanisms, such as TLS. The organization utilizes CMS-approved encryption
	ethods, in combination with certificate-based authentication or additional authenti	
Test: Information system to det	ermine if the organization enables and forces use of application security mechar bination with certificate-based authentication or additional authentication protecti	nisms, such as TLS. The organization utilizes CMS-approved encryption and password
		ion (e.g., token-based, biometric).
SC-CMS-3(CMS-1) – Enhancen	lent (Figh)	
Control		
	nd implemented, refer to ARS Appendix A for e-Authentication Standards contro	
	References: ARS: SC-CMS-3(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: \$	3C-CMS-3(CMS-1).1	
Assessment Objective		
0	at uses e-authentication is required to refer to ARS Appendix A for e-Authentication	tion Standards controls and procedures.
Assessment Methods And Obj		
		such as TLS, and utilizing minimum encryption and password authentication although,
no specific requirements are ma	,	
a 1	0 11	l, such as TLS, and utilizing minimum encryption and password authentication although
no specific requirements are ma		environization utilized minimum operation and personal outbestication of the use as
specific requirements are mand		rganization utilizes minimum encryption and password authentication although, no
SC-CMS-4 – Electronic Mail		
	(nigii)	
Control	even and and implemented affectively to material OMC constitive information the	
	cumented, and implemented effectively to protect CMS sensitive information that	at is sent via e-mail.
Guidance	has shale for her all an even the information of a second to the NUCT OD	
<u> </u>	I controls for handling sensitive information via e-mail is the NIST SP. References: ARS: SC-CMS-4; PISP: 4.16.27	Delete d Os strade
		Related Controls:
ASSESSMENT PROCEDURE: \$	5C-CMS-4.1	
Assessment Objective		
	fectively develops, documents, and implements protections for CMS sensitive in	formation that is sent via e-mail.
Assessment Methods And Obj		
	termine if all e-mail messages with CMS sensitive information are transmitted us	
	onnel to determine if all e-mail messages with CMS sensitive information is prote	ected, controlled, and monitored.
SC-CMS-4(CMS-0) – Enhancen	hent (High)	
Control		
	all CMS sensitive information in an encrypted attachment.	
Applicability: All	References: ARS: SC-CMS-4(CMS-0); IRS-1075: 5.7.3#1	Related Controls:
ASSESSMENT PROCEDURE: \$	3C-CMS-4(CMS-0).1	
Assessment Objective		
Determine if the organization m		requirements as prescribed in this amplifying enhancement to the baseline control.
		requirements as prescribed in this amplifying enhancement to the baseline control.

Interview: Organizational	personnel to determine if all e-mail messages are encrypted, and encryption /decryption for received	messages
SC-CMS-5 – Persistent		111633ayes.
Control		
The use of persistent cook	ties on a CMS web site is prohibited unless explicitly approved in writing by the DHHS Secretary.	
Guidance		
Requests to DHHS should		
Applicability: All	References: ARS: SC-CMS-5; PISP: 4.16.28	Related Controls:
ASSESSMENT PROCEDU	RE: SC-CMS-5.1	
Assessment Objective		
Determine if the organizati	ion does not use a persistent cookie configuration on a CMS web site to remember subsequent visits	unless approved in writing by the DHHS Secretary.
Assessment Methods And	Objects	
	aseline and change management documentation for configurations using persistent cookies.	
	nistrators to determine if the CMS web site has persistent cookies enable in the baseline configuration	n or have written approval to enable persistent cookies from the DHHS
Secretary.		
SC-CMS-6 – Network In	terconnection (High)	
Control		
Controls shall be develope	ed, documented, and implemented effectively to ensure that only properly authorized network intercor	nnections external to the system boundaries are established.
Guidance		
A good place to obtain tec	hnical controls for securing interconnections external to the system boundaries is the NIST SP.	
Applicability: All	References: ARS: SC-CMS-6; PISP: 4.16.29	Related Controls:
ASSESSMENT PROCEDU	RE: SC-CMS-6.1	
Assessment Objective		
Determine if the organizati	ion effectively documents and implements authorized network interconnections external to the system	n boundaries.
Assessment Methods And	Objects	
Examine: Documentation	to determine remote location(s) follow all CMS IS policies and standards for all external interconnecti	ions.
SC-CMS-6(CMS-0) - Enhai	ncement (High)	
Control		
Ensure remote location(s)	(e.g., users and sites using a network interconnection external to the system boundaries) follow all C	CMS IS policies and standards and obtain a signed Interconnection
Security Agreement. Docu	ument the interconnection in the SSP for the system that is connected to the remote location.	, č
Applicability: All	References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2	Related Controls:
ASSESSMENT PROCEDU	RE: SC-CMS-6(CMS-0).1	
Assessment Objective		
Determine if the organizati	ion meets the requirements as specified in the baseline control and the specific CMS requirements as	s prescribed in this amplifying enhancement to the baseline control.
Assessment Methods And	Objects	· · · -
	to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Intercon	nnection Security Agreement. Document the interconnection in the
	connected to the remote location.	
	etermine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnec	ction Security Agreement. Document the interconnection in the SSP for
the system that is connect	ed to the remote location.	

System and Information Integrity (SI) – Operational

SI-1 – System and Information Integrity Policy and Procedures (High)

Control

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems, software, and information. The procedures and automated mechanisms shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. It is good practice to have an automated system which is host based to automatically detect, block/filter and alert supervisors or managers that possible unauthorized changes to software and the information system have occurred.

Applicability: All References: ARS: SI-1; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-1; PISP: 4.17.1 Related Controls:	PISP: 4 17 1	
---	--------------	--

ASSESSMENT PROCEDURE: SI-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents system and information integrity policy and procedures;

(ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and information integrity policy and procedures; and

(iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and information integrity responsibilities.

ASSESSMENT PROCEDURE: SI-1.2

Assessment Objective

Determine if:

(i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with system and information integrity responsibilities.

SI-2 – Flaw Remediation (High)

Control

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. The flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

Guidance

The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. It is a good practice to test the changes in a laboratory environment on like systems prior to approving and implementing the updates and changes. NIST SP 800-40, provides guidance on security patch installation and patch management.

Applicability: All References: ARS: SI-2; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2; PISP: 4.17.2 Related Cont 3, IR-4, SI-17	s: CA-2, CA-4, CA-7, CM-
---	--------------------------

ASSESSMENT PROCEDURE: SI-2.1

Assessment Objective

Determine if:

(i) the organization identifies, reports, and corrects information system flaws;

(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;

(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;

(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and

(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(0) – Enhancement (High)

Control

Correct identified information system flaws on production equipment within 72 hours.

(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and

(b) Manage the flaw remediation process centrally.

	Applicability: A	All .		References: ARS: SI-2(0); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2; PISP: 4.17.2	Related Controls:
--	------------------	-------	--	---	-------------------

ASSESSMENT PROCEDURE: SI-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(1) – Enhancement (High)

Control

Updates are installed automatically.

2(1)	2(1)	Applicability: All	References: ARS: SI-2(1); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2(1)	Related Controls:
------	------	--------------------	---	-------------------

ASSESSMENT PROCEDURE: SI-2(1).1

Assessment Objective

Determine if the organization centrally manages the flaw remediation process and installs updates automatically.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records.

Test: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates.

SI-2(2) – Enhancement (High)

Control

Employ automated mechanisms periodically an	d upon demand to determine the state of information system components with regard to flaw remediation.	
Applicability: All	References: ARS: SI-2(2); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-	Related Controls:

	2(2)	
ASSESSMENT PROCEDURE: SI-2(2).1		
Assessment Objective		
Determine if the organization employs automate	I mechanisms to periodically and upon demand determine the state of information system components v	with regard to flaw remediation.
Assessment Methods And Objects		-
information system configuration settings and as	r; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information actions proceeded documentation; list of information system flaws; list of recent security flaw remediation actions proceeded actions	
information system audit records; other relevant		
Test: Automated mechanisms implementing info		
SI-3 – Malicious Code Protection (High)		
Control		
effectively to identify and isolate suspected malic workstation, server, or mobile computing device	is that include a capability of automatic updates shall be in place and supporting procedures shall be de- ious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical informa on the network to detect and eradicate malicious code transported by email, email attachments, removal multiple vendors, if possible, and update virus protection mechanisms whenever new releases are avai	tion system entry points, and at each ble media or other methods. Business
Guidance		
servers) and at workstations, servers, or mobile viruses, worms, Trojan horses, spyware) transpo common means; or (ii) by exploiting information are available in accordance with organizational of (e.g., using one vendor for boundary devices and	ion mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail server computing devices on the network. The organization uses the malicious code protection mechanisms to rted: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB or system vulnerabilities. The organization updates malicious code protection mechanisms (including the la ponfiguration management policy and procedures. The organization considers using malicious code prote servers and another vendor for workstations). The organization also considers the receipt of false posit the availability of the information system. NIST SP 800-83 provides guidance on implementing malicious	detect and eradicate malicious code (e.g., devices, diskettes or compact disks), or other ttest virus definitions) whenever new releases ection software products from multiple vendors tives during malicious code detection and
Applicability: All	References: ARS: SI-3; FISCAM: TCC-1.3.2; IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	Related Controls:
ASSESSMENT PROCEDURE: SI-3.1		
Assessment Objective		
Determine if:		
(i) the information system implements malicious	code protection;	
 (ii) the organization employs malicious code prot and eradicate malicious code; 	ection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile	e computing devices on the network to detect
 (iii) the malicious code protection mechanisms d means, or by exploiting information system vulne 	etect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet a rabilities:	ccess, removable media, or other common
	ection mechanisms whenever new releases are available; and	
	e appropriately updated to include the latest malicious code definitions, configured to perform periodic so	cans of the information system as well as real-
	les are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.	
Assessment Methods And Objects		
	r; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechar	nisms; records of malicious code protection
	s and associated documentation; other relevant documents or records.	
SI-3(0) – Enhancement (High)		
Control		
	on system entry points, including firewalls, email servers, remote access servers, workstations, servers,	and mobile computing devices by employing
	nalicious code transported by email, email attachments, and removable media.	Deleted Controles
	References: ARS: SI-3(0); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	Related Controls:
ASSESSMENT PROCEDURE: SI-3(0).1		
Assessment Objective Determine if the organization meets the requirem	ents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ving enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(1) – Enhancement (High) Control Manage and update malicious code protection software centrally with automatic updates for the latest malicious code definitions whenever new releases are available. Applicability: All References: ARS: SI-3(1); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3(1) **Related Controls:** ASSESSMENT PROCEDURE: SI-3(1).1 **Assessment Objective** Determine if the organization centrally manages malicious code protection mechanisms. **Assessment Methods And Objects** Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records. SI-3(2) – Enhancement (High) Control Employ automated mechanisms to update malicious code protection. Applicability: All References: ARS: SI-3(2); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3(2) **Related Controls: ASSESSMENT PROCEDURE: SI-3(2).1 Assessment Objective** Determine if the organization automatically updates malicious code protection mechanisms. Assessment Methods And Objects Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records. Test: Automatic update capability for malicious code protection. SI-3(CMS-1) – Enhancement (High) Control Enable real-time file scanning. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and every twelve (12) hours. Applicability: All References: ARS: SI-3(CMS-1): IRS-1075; 5.6.2.5#1.3 **Related Controls:** ASSESSMENT PROCEDURE: SI-3(CMS-1).1 **Assessment Objective** Determine if: (i) real-time file scanning is enabled; (ii) real-time desktop malicious code scanning is enabled and monitored; and (iii) software is configured to perform critical system file scans during system boot and every twelve (12) hours. **Assessment Methods And Objects** Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records to determine real-time file scanning is enabled. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and every twelve (12) hours. Interview: Personnel with system and information integrity responsibilities to determine real-time file scanning is enabled, desktop malicious code scanning software is installed, real-time protection, and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and every twelve (12) hours. Test: Information system real-time file scanning is enabled, desktop malicious code scanning software is installed, real-time protection, and monitoring is enabled, and the software is configured to perform critical system file scans during system boot and every twelve (12) hours. SI-4 – Information System Monitoring Tools and Techniques (High) Control

Effective monitoring tools and techniques providing real-time identification of unauthorized use, misuse, and abuse of the information system shall be implemented.

Guidance

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system monitoring activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information, system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST SP 800-61 provides guidance on detecting malware-based attacks through malicious code protection software. NIST SP 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST SP 800-94 provides guidance on intrusion detection and prevention.

A second se	dance on intrusion detection and prevention.	
Applicability: All	References: ARS: SI-4; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800- 53/53A: SI-4; PISP: 4.17.4	Related Controls: AC-8, AU-4, CM-6
ASSESSMENT PROCEDURE:	SI-4.1	
Assessment Objective		
Determine if the organization e	employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of un	authorized use of the system.
Assessment Methods And Ob	ojects	
	ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desi es documentation; information system configuration settings and associated documentation; other relevant documents or	
SI-4(1) – Enhancement (High)		
Control		
Connect individual IDS device	s to a common IDS management network using common protocols.	
Applicability: All	References: ARS: SI-4(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(1)	Related Controls:
ASSESSMENT PROCEDURE:	SI-4(1).1	
Assessment Objective		
•	interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using comm	ion protocols.
Assessment Methods And Ok		
	ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desi	an documentation: information system
	es documentation; information system configuration settings and associated documentation; information system protocols	
records.(Optional)		
	e intrusion detection capability.(Optional)	
CL (/2) Enhancement (Lligh)		
SI-4(2) – Ennancement (High)		
SI-4(2) – Enhancement (High) Control Employ automated information	n system monitoring tools to support near-real-time analysis of events.	
Control Employ automated information		Related Controls:
Control	n system monitoring tools to support near-real-time analysis of events. References: ARS: SI-4(2); NIST 800-53/53A: SI-4(2)	Related Controls:
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE:	n system monitoring tools to support near-real-time analysis of events. References: ARS: SI-4(2); NIST 800-53/53A: SI-4(2)	Related Controls:
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective	n system monitoring tools to support near-real-time analysis of events.	Related Controls:
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization e	n system monitoring tools to support near-real-time analysis of events.	Related Controls:
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ot	n system monitoring tools to support near-real-time analysis of events.	
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ot Examine: System and information	system monitoring tools to support near-real-time analysis of events. References: ARS: SI-4(2); NIST 800-53/53A: SI-4(2) SI-4(2).1 employs automated tools to support near-real-time analysis of events. bjects	gn documentation; information system
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ot Examine: System and information monitoring tools and technique records.	A system monitoring tools to support near-real-time analysis of events. References: ARS: SI-4(2); NIST 800-53/53A: SI-4(2) SI-4(2).1 employs automated tools to support near-real-time analysis of events. bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desi es documentation; information system configuration settings and associated documentation; information system protocols	gn documentation; information system
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ot Examine: System and informat monitoring tools and technique records. Test: Automated tools support	system monitoring tools to support near-real-time analysis of events. References: ARS: SI-4(2); NIST 800-53/53A: SI-4(2) SI-4(2).1 employs automated tools to support near-real-time analysis of events. bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desi es documentation; information system configuration settings and associated documentation; information system protocols ting near real-time event analysis.	gn documentation; information system
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ot Examine: System and information monitoring tools and technique records.	system monitoring tools to support near-real-time analysis of events. References: ARS: SI-4(2); NIST 800-53/53A: SI-4(2) SI-4(2).1 employs automated tools to support near-real-time analysis of events. bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desi es documentation; information system configuration settings and associated documentation; information system protocols ting near real-time event analysis.	gn documentation; information system
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ot Examine: System and informat monitoring tools and technique records. Test: Automated tools support	system monitoring tools to support near-real-time analysis of events. References: ARS: SI-4(2); NIST 800-53/53A: SI-4(2) SI-4(2).1 employs automated tools to support near-real-time analysis of events. bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desi es documentation; information system configuration settings and associated documentation; information system protocols ting near real-time event analysis.	gn documentation; information system
Control Employ automated information Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ob Examine: System and informat monitoring tools and technique records. Test: Automated tools support SI-4(3) – Enhancement (High) Control	system monitoring tools to support near-real-time analysis of events. References: ARS: SI-4(2); NIST 800-53/53A: SI-4(2) SI-4(2).1 employs automated tools to support near-real-time analysis of events. bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desi es documentation; information system configuration settings and associated documentation; information system protocols ting near real-time event analysis.	gn documentation; information system documentation; other relevant documents o

	il-4(3).1	
Assessment Objective		
Determine if the organization err	ploys automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid re of attack isolation and elimination.	esponse to attacks by enabling reconfiguration
Assessment Methods And Obje		
Examine: System and information	on integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system configuration settings and associated documentation; information system protocols	
Test: Automated tools supportin	g the integration of intrusion detection tools and access/flow control mechanisms.(Optional)	
SI-4(4) – Enhancement (High)		
Control		
Monitor inbound and outbound c	ommunications for unusual or unauthorized activities or conditions.	
Guidance		
	or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling	
Applicability: All	References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4)	Related Controls:
ASSESSMENT PROCEDURE: S	I-4(4).1	
Assessment Objective		
Determine if:	turned of activities or conditions considered unusual or unsutherized, and	
0	types of activities or conditions considered unusual or unauthorized; and ors inbound and outbound communications for unusual or unauthorized activities or conditions.	
Assessment Methods And Obje		
	on integrity policy; procedures addressing information system monitoring tools and techniques; types of activities or con	ditions considered unusual or unauthorized:
	ools and techniques documentation; information system configuration settings and associated documentation; other rele	
Test: Information system monito	ring capability for inbound and outbound communications.	
SI-4(5) – Enhancement (High)		
Control		
(a) Presence of malicious code,	en indications of the following types of compromise, or potential compromise, occur:	
(b) Unauthorized export of inform		
(c) Signaling to an external inform		
(d) Potential intrusions.	mation system, or	Polated Controls
(d) Potential intrusions. Applicability: All	mation system, or References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5)	Related Controls:
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S	mation system, or References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5)	Related Controls:
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective	mation system, or References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5)	Related Controls:
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if:	mation system, or References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5) SI-4(5).1	Related Controls:
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if: (i) the organization identifies indi	References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5) SI-4(5).1 Iccations of compromise or potential compromise to the security of the information system; and	Related Controls:
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if: (i) the organization identifies indi (ii) the information system provid	References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5) SI-4(5).1 Ications of compromise or potential compromise to the security of the information system; and les a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur.	Related Controls:
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if: (i) the organization identifies indi (ii) the information system provic Assessment Methods And Obje Examine: System and information	References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5) SI-4(5).1 Ications of compromise or potential compromise to the security of the information system; and les a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur.	
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if: (i) the organization identifies indi (ii) the information system provic Assessment Methods And Obje Examine: System and information	References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5) SI-4(5).1 Iccations of compromise or potential compromise to the security of the information system; and les a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ects on integrity policy; procedures addressing information system monitoring tools and techniques; information system security formation system configuration settings and associated documentation; other relevant documents or records.	
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if: (i) the organization identifies indi (ii) the information system provic Assessment Methods And Obje Examine: System and information and techniques documentation; Test: Information system monitor	References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5) SI-4(5).1 Iccations of compromise or potential compromise to the security of the information system; and les a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ects on integrity policy; procedures addressing information system monitoring tools and techniques; information system security information system configuration settings and associated documentation; other relevant documents or records. ring real-time alert capability.	
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if: (i) the organization identifies indi (ii) the information system provic Assessment Methods And Obje Examine: System and information and techniques documentation; Test: Information system monitor	References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5) SI-4(5).1 Iccations of compromise or potential compromise to the security of the information system; and les a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ects on integrity policy; procedures addressing information system monitoring tools and techniques; information system security information system configuration settings and associated documentation; other relevant documents or records. ring real-time alert capability.	
(d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: S Assessment Objective Determine if: (i) the organization identifies indi (ii) the information system provid Assessment Methods And Obje Examine: System and informatio and techniques documentation; i Test: Information system monito SI-4(CMS-1) – Enhancement (H Control	References: ARS: SI-4(5); NIST 800-53/53A: SI-4(5) SI-4(5).1 Iccations of compromise or potential compromise to the security of the information system; and les a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ects on integrity policy; procedures addressing information system monitoring tools and techniques; information system security information system configuration settings and associated documentation; other relevant documents or records. ring real-time alert capability.	

ASSESSMENT PROCEDURE: SI-4(CMS-1).1

Assessment Objective

Determine if:

(i) IDS devices are installed at network perimeter points; and

(ii) host-based IDS sensors are installed on critical servers.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

Interview: Personnel with system and information integrity responsibilities to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

Test: Information system-wide intrusion detection capability to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

SI-5 – Security Alerts and Advisories (High)

Control

Procedures shall be developed, documented, and implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis, and for issuing IS alerts and advisories to appropriate personnel. Upon receipt of such alerts and advisories, personnel shall take appropriate response actions. The types of actions to be taken in response to security alerts / advisories shall be documented.

Guidance

The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST SP 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Applicability: All	References: ARS: SI-5; NIST 800-53/53A: SI-5; PISP: 4.17.5	Related Controls:
ASSESSMENT PROCEDURE: SI-5.1		

Assessment Objective

Determine if:

(i) the organization receives information system security alerts/advisories on a regular basis;

(ii) the organization issues security alerts/advisories to appropriate organizational personnel; and

(iii) the organization takes appropriate actions in response to security alerts/advisories.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; NIST SP 800-40; records of security alerts and advisories; other relevant documents or records.

Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system.

SI-5(1) – Enhancement (High)

Control

Employ automated mechanisms to make security alerts and advisory information available to all appropriate personnel.

	······································	
Applicability: All	References: ARS: SI-5(1); NIST 800-53/53A: SI-5(1)	Related Controls:
ASSESSMENT PROCEDURE: SI-5(1).1		

Assessment Objective

Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records.

Test: Automated mechanisms implementing the distribution of security alert and advisory information.

SI-6 – Security Functionality Verification (High)

Control

Automated mechanisms shall be established and implemented effectively to provide the capability for CMS information systems to verify the correct operation of security functions on a regular basis,

,	actions when security-related anomalies are discovered.	
Guidance		
	to all security functions. For those security functions that are not able to execute auto	mated self-tests, the organization either implements
	epts the risk of not performing the verification as required.	1
Applicability: All	References: ARS: SI-6; NIST 800-53/53A: SI-6; PISP: 4.17.6	Related Controls:
ASSESSMENT PROCEDURE: SI-6.1		
Assessment Objective		
Determine if:		
() 0 11 1	ditions for conducting security function verification;	
	y function verification, the frequency of the verifications;	
	responses to anomalies discovered during security function verification;	
verification); and	peration of security functions in accordance with organization-defined conditions and	in accordance with organization-defined frequency (if periodic
	function anomalies in accordance with organization-defined responses.	
Assessment Methods And Objects		
	cy; procedures addressing security function verification; information system design do ocumentation; other relevant documents or records.	ocumentation; information system security plan; information
SI-6(0) – Enhancement (High)		
Control		
	Ily verify the correct operation of system security functions upon system startup and r	estart, upon command by users with appropriate access, and a
	stem administration upon detection of security anomalies.	
Applicability: All	References: ARS: SI-6(0); NIST 800-53/53A: SI-6; PISP: 4.17.6	Related Controls:
ASSESSMENT PROCEDURE: SI-6(0).1	· · · ·	
Assessment Objective		
Determine if the organization meets the require	ments as specified in the baseline control and the specific CMS requirements as pres	scribed in this amplifying enhancement to the baseline control.
o 1	ments as specified in the baseline control and the specific CMS requirements as pres	scribed in this amplifying enhancement to the baseline control.
Assessment Methods And Objects		
Assessment Methods And Objects Examine: System and information integrity poli- defined conditions for conducting security function	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per	ocumentation; information system security plan (for organization riodic), and organization-defined information system responses
Assessment Methods And Objects Examine: System and information integrity poli- defined conditions for conducting security functi security function anomalies); information system	cy; procedures addressing security function verification; information system design do	ocumentation; information system security plan (for organization riodic), and organization-defined information system responses t
Assessment Methods And Objects Examine: System and information integrity poli- defined conditions for conducting security functi security function anomalies); information system Test: Security function verification capability.	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per	ocumentation; information system security plan (for organization riodic), and organization-defined information system responses t
Assessment Methods And Objects Examine: System and information integrity polid defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High)	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per	ocumentation; information system security plan (for organization riodic), and organization-defined information system responses t
Assessment Methods And Objects Examine: System and information integrity polid defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per n configuration settings and associated documentation; other relevant documents or r	ocumentation; information system security plan (for organization riodic), and organization-defined information system responses t
Assessment Methods And Objects Examine: System and information integrity polid defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide cent	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per n configuration settings and associated documentation; other relevant documents or r	pocumentation; information system security plan (for organization iodic), and organization-defined information system responses t records.
Assessment Methods And Objects Examine: System and information integrity polid defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide cent Applicability: All	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per n configuration settings and associated documentation; other relevant documents or r	ocumentation; information system security plan (for organization riodic), and organization-defined information system responses t
Assessment Methods And Objects Examine: System and information integrity polition defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide cent Applicability: All ASSESSMENT PROCEDURE: SI-6(1).1	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per n configuration settings and associated documentation; other relevant documents or r	ocumentation; information system security plan (for organization iodic), and organization-defined information system responses t records.
Assessment Methods And Objects Examine: System and information integrity polition defined conditions for conducting security function system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide cent Applicability: All ASSESSMENT PROCEDURE: SI-6(1).1 Assessment Objective	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per n configuration settings and associated documentation; other relevant documents or r tralized notification of failed automated security tests. References: ARS: SI-6(1); NIST 800-53/53A: SI-6(1)	pocumentation; information system security plan (for organization iodic), and organization-defined information system responses records.
Assessment Methods And Objects Examine: System and information integrity polition defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide cent Applicability: All ASSESSMENT PROCEDURE: SI-6(1).1 Assessment Objective Determine if the organization employs automated	cy; procedures addressing security function verification; information system design do on verification, organization-defined frequency of security function verifications (if per n configuration settings and associated documentation; other relevant documents or r	ocumentation; information system security plan (for organization iodic), and organization-defined information system responses records.
Assessment Methods And Objects Examine: System and information integrity politive defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide center of the system of th	cy; procedures addressing security function verification; information system design do ion verification, organization-defined frequency of security function verifications (if per in configuration settings and associated documentation; other relevant documents or r tralized notification of failed automated security tests. References: ARS: SI-6(1); NIST 800-53/53A: SI-6(1) ed mechanisms to provide notification of failed security tests.	Decumentation; information system security plan (for organization- riodic), and organization-defined information system responses records.
Assessment Methods And Objects Examine: System and information integrity polition defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide cent Applicability: All ASSESSMENT PROCEDURE: SI-6(1).1 Assessment Objective Determine if the organization employs automate Assessment Methods And Objects Examine: System and information integrity policity	cy; procedures addressing security function verification; information system design do ion verification, organization-defined frequency of security function verifications (if per in configuration settings and associated documentation; other relevant documents or r tralized notification of failed automated security tests. References: ARS: SI-6(1); NIST 800-53/53A: SI-6(1) ed mechanisms to provide notification of failed security tests. cy; procedures addressing security function verification; information system design do	Decumentation; information system security plan (for organization- riodic), and organization-defined information system responses records.
Assessment Methods And Objects Examine: System and information integrity polition defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide cent Applicability: All ASSESSMENT PROCEDURE: SI-6(1).1 Assessment Objective Determine if the organization employs automate Assessment Methods And Objects Examine: System and information integrity polition system configuration settings and associated do	cy; procedures addressing security function verification; information system design do ion verification, organization-defined frequency of security function verifications (if per in configuration settings and associated documentation; other relevant documents or r itralized notification of failed automated security tests. References: ARS: SI-6(1); NIST 800-53/53A: SI-6(1) ed mechanisms to provide notification of failed security tests. cy; procedures addressing security function verification; information system design do bocumentation; other relevant documents or records.(Optional)	Decumentation; information system security plan (for organization- riodic), and organization-defined information system responses records.
Assessment Methods And Objects Examine: System and information integrity polition defined conditions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide cent Applicability: All ASSESSMENT PROCEDURE: SI-6(1).1 Assessment Objective Determine if the organization employs automate Assessment Methods And Objects Examine: System and information integrity polition system configuration settings and associated do Test: Automated mechanisms implementing allow	cy; procedures addressing security function verification; information system design do ion verification, organization-defined frequency of security function verifications (if per in configuration settings and associated documentation; other relevant documents or r tralized notification of failed automated security tests. References: ARS: SI-6(1); NIST 800-53/53A: SI-6(1) ed mechanisms to provide notification of failed security tests. cy; procedures addressing security function verification; information system design do	Decumentation; information system security plan (for organization- riodic), and organization-defined information system responses records.
Assessment Methods And Objects Examine: System and information integrity politions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide centres Assessment Objective Determine if the organization employs automated Assessment Methods And Objects Examine: System and information integrity politions system configuration settings and associated dor Test: Automated mechanisms implementing allows SI-6(2) – Enhancement (High)	cy; procedures addressing security function verification; information system design do ion verification, organization-defined frequency of security function verifications (if per in configuration settings and associated documentation; other relevant documents or r itralized notification of failed automated security tests. References: ARS: SI-6(1); NIST 800-53/53A: SI-6(1) ed mechanisms to provide notification of failed security tests. cy; procedures addressing security function verification; information system design do bocumentation; other relevant documents or records.(Optional)	Decumentation; information system security plan (for organization- riodic), and organization-defined information system responses records.
Assessment Methods And Objects Examine: System and information integrity politions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide centres Applicability: All ASSESSMENT PROCEDURE: SI-6(1).1 Assessment Objective Determine if the organization employs automate Assessment Methods And Objects Examine: System and information integrity politions system configuration settings and associated dor Test: Automated mechanisms implementing allows SI-6(2) – Enhancement (High) Control	cy; procedures addressing security function verification; information system design do ion verification, organization-defined frequency of security function verifications (if per in configuration settings and associated documentation; other relevant documents or r tralized notification of failed automated security tests. References: ARS: SI-6(1); NIST 800-53/53A: SI-6(1) ed mechanisms to provide notification of failed security tests. cy; procedures addressing security function verification; information system design do ocumentation; other relevant documents or records.(Optional) erts and/or notifications for failed automated security tests.(Optional)	coumentation; information system security plan (for organization riodic), and organization-defined information system responses t records.
Assessment Methods And Objects Examine: System and information integrity politions for conducting security function security function anomalies); information system Test: Security function verification capability. SI-6(1) – Enhancement (High) Control Employ automated mechanisms to provide centres Applicability: All ASSESSMENT PROCEDURE: SI-6(1).1 Assessment Objective Determine if the organization employs automate Assessment Methods And Objects Examine: System and information integrity politis system configuration settings and associated dor Test: Automated mechanisms implementing allows SI-6(2) – Enhancement (High) Control	cy; procedures addressing security function verification; information system design do ion verification, organization-defined frequency of security function verifications (if per in configuration settings and associated documentation; other relevant documents or r itralized notification of failed automated security tests. References: ARS: SI-6(1); NIST 800-53/53A: SI-6(1) ed mechanisms to provide notification of failed security tests. cy; procedures addressing security function verification; information system design do bocumentation; other relevant documents or records.(Optional)	Decumentation; information system security plan (for organization- riodic), and organization-defined information system responses records.

ASSESSMENT PROCEDURE: SI-6(2).1 Assessment Objective Determine if the organization employs automated mechanisms to support management of distributed security testing. **Assessment Methods And Objects** Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan; information system configuration settings and associated documentation: other relevant documents or records.(Optional) Test: Automated mechanisms supporting the management of distributed security function testing.(Optional) SI-7 – Software and Information Integrity (High) Control Automated mechanisms for software and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to software. Good software engineering practices consistent with CMS IS policy and procedures shall be employed with regard to commercial-off-the-shelf (COTS) integrity mechanisms, and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications. Guidance The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cvclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts. References: ARS: SI-7: FISCAM: TAN-3.1.2. TAN-3.2.1. TAN-3.2.2. TAY-2.1.4. TAY-2.2.2. TCP-Applicability: All **Related Controls:** 2.1.2, TCP-2.1.3, TCP-2.1.4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7; PISP: 4.17.7 **ASSESSMENT PROCEDURE: SI-7.1** Assessment Objective Determine if: (i) the information system detects and protects against unauthorized changes to software and information; and (ii) the organization employs effective integrity verification tools in accordance with good software engineering practices. **Assessment Methods And Objects** Examine: System and information integrity policy: procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records. Test: Software integrity protection and verification capability. SI-7(0) – Enhancement (High) Control Employ off-the-shelf integrity mechanisms such as parity checks, check-sums, error detection data validation techniques, cyclical redundancy checks, and cryptographic hashes to detect and protect against information tampering, errors, omissions and unauthorized changes to software and use tools to automatically monitor the integrity of the information system and the application it hosts. Applicability: All References: ARS: SI-7(0); FISCAM: TAC-3.3; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-**Related Controls:** 53/53A: SI-7: PISP: 4.17.7 ASSESSMENT PROCEDURE: SI-7(0).1 **Assessment Objective** Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation: integrity verification tools and applications documentation: other relevant documents or records. Test: Software integrity protection and verification capability. SI-7(1) – Enhancement (High) Control Perform weekly integrity scans of the system. Applicability: All References: ARS: SI-7(1); HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7(1) **Related Controls:**

ASSESSMENT PROCEDURE: SI-7(1).1		
Assessment Objective		
Determine if:		
(i) the organization defines the frequency of inte		
(ii) the organization reassesses the integrity of s	oftware and information by performing integrity scans of the information system in accordance with the	organization-defined frequency.
Assessment Methods And Objects		
	cy; procedures addressing software and information integrity; information system security plan; informat	ion system configuration settings and
	tools and applications documentation; records of integrity scans; other relevant documents or records.	
SI-7(2) – Enhancement (High)		
Control		
	to appropriate individuals upon discovering discrepancies during integrity verification.	
Applicability: All	References: ARS: SI-7(2); HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7(2)	Related Controls:
ASSESSMENT PROCEDURE: SI-7(2).1		
Assessment Objective		
Determine if the organization employs automate	d tools that provide notification to appropriate individuals upon discovering discrepancies during integrit	y verification.
Assessment Methods And Objects		
Examine: System and information integrity polic	cy; procedures addressing software and information integrity; information system configuration settings	and associated documentation; integrity
	n; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepanci	es; other relevant documents or records.
SI-7(FIS-1) – Enhancement (High)		
Control		
A comprehensive set of test transactions and da	ata is developed that represents the various activities and conditions that will be encountered in process	ing. Live data are not used in testing of
program changes except to build test data files.		
Applicability: All	References: FISCAM: TCC-2.1.6, TCC-2.1.7	Related Controls:
Applicability: All	References: FISCAM: TCC-2.1.6, TCC-2.1.7	Related Controls:
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1	References: FISCAM: TCC-2.1.6, TCC-2.1.7	Related Controls:
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1	References: FISCAM: TCC-2.1.6, TCC-2.1.7	Related Controls:
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so	et of test transactions and data is developed that represents the various activities and conditions that wi	
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live		
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects	et of test transactions and data is developed that represents the various activities and conditions that wi	
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures.	et of test transactions and data is developed that represents the various activities and conditions that wi	
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive s (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data.	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files.	
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive si (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files.	
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High)	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files.	
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files.	ill be encountered in processing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals est	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files. assurance personnel. stablished over source documents are used to help determine the completeness of data entry and proce	ill be encountered in processing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals ex Applicability: All; Optional for CWF, DC, EDC, SS	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files.	ill be encountered in processing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals ex Applicability: All; Optional for CWF, DC, EDC, SS	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files. assurance personnel. stablished over source documents are used to help determine the completeness of data entry and proce	ill be encountered in processing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals en Assessment PROCEDURE: SI-7(FIS-2).1 Assessment Objective	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files. assurance personnel. stablished over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1	essing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals end Assessment Objective Determine if the organizational user-prepared record rec	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files. assurance personnel. stablished over source documents are used to help determine the completeness of data entry and proce	essing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals end ASSESSMENT PROCEDURE: SI-7(FIS-2).1 Assessment Objective Determine if the organizational user-prepared record r	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files. assurance personnel. stablished over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1	essing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals end ASSESSMENT PROCEDURE: SI-7(FIS-2).1 Assessment Objective Determine if the organizational user-prepared record counts Assessment Methods And Objects Examine: Activity for developing record counts	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files. assurance personnel. stablished over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1	essing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive si (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals ei Applicability: All; Optional for CWF, DC, EDC, SS ASSESSMENT PROCEDURE: SI-7(FIS-2).1 Assessment Methods And Objects Examine if the organizational user-prepared record counts Examine: Activity for developing record counts Examine: Application documentation.	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files. assurance personnel. stablished over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1	essing.
Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS-1).1 Assessment Objective Determine if: (i) the organization provides a comprehensive so (ii) the organizational validation does not use live Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Test transactions and data. Interview: Programmers, auditors, and quality a SI-7(FIS-2) – Enhancement (High) Control User-prepared record count and control totals ei Applicability: All; Optional for CWF, DC, EDC, SS ASSESSMENT PROCEDURE: SI-7(FIS-2).1 Assessment Methods And Objects Examine if the organizational user-prepared record counts	et of test transactions and data is developed that represents the various activities and conditions that wi e data in testing of program changes except to build test data files. assurance personnel. stablished over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1	essing.

SI-7(FIS-3) – Enhancement (High)		
Control		
	ount and control totals are accumulated progressively for a specific time r	period (daily or more frequently) and are used to help determine the completeness
or data entry and processing.		
Applicability: All; Optional for CWF	References: FISCAM: TCP-1.1.2	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-		
Assessment Objective	<u>· /</u>	
Determine if the organizational on-line or determine the completeness or data entry		ressively for a specific time period (daily or more frequently) and are used to help
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Pertinent policies and procedur	'es.	
Examine: Supporting documentation gen		
Interview: Application programmer, if ava		
Interview: User management and person		
SI-7(FIS-4) – Enhancement (High)		
Control		
Record counts and control totals are estal	blished over and entered with transaction data, and reconciled to determi	ine the completeness of data entry.
Applicability: All	References: FISCAM: TCP-2.1.1	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-		
Assessment Objective	·	
Determine if the organizational record cou	ints and control totals are established over and entered with transaction o	data, and reconciled to determine the completeness of data entry.
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Pertinent policies and procedu	'es	
Examine: Reconciliation activities.		
Interview: Data control personnel.		
Interview: User management and person	nel	
SI-7(FIS-5) – Enhancement (High)		
Control		
	ne the completeness of transactions processed, master files updated, and	d outputs generated.
Applicability: All	References: FISCAM: TCP-2.2.1	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-	5).1	
Assessment Objective		
Determine if the organizational reconciliat	ions are performed to determine the completeness of transactions proces	ssed, master files updated, and outputs generated.
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Pertinent policies and procedu	'es	
Examine: Reconciliation activities.		
Interview: Data control personnel.		
Interview: User management and person	nel	
SI-8 – Spam Protection (High)		
Control		
	on shall be in place at critical information system ontry points, workstation	no convers and mobile computing devices on the naturally Conserting presedures
		ons, servers, and mobile computing devices on the network. Supporting procedures
snall be developed, documented, and imp	lemented effectively to both protect against and detect spam.	

Guidance		
The organization employs spam protection mec	hanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access	s servers) and at workstations, servers, or
	organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited	
	or other common means. Consideration is given to using spam protection software products from multip	le vendors (e.g., using one vendor for
	dor for workstations). NIST SP 800-45 provides guidance on electronic mail security.	
Applicability: All	References: ARS: SI-8; HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8; PISP: 4.17.8	Related Controls:
ASSESSMENT PROCEDURE: SI-8.1		
Assessment Objective		
Determine if:		
(i) the information system implements spam pro	vtection;	
	echanisms at critical information system entry points and at workstations, servers, or mobile computing of	
	nechanisms to detect and take appropriate action on unsolicited messages transported by electronic mai	
	nechanisms whenever new releases are available in accordance with organizational policy and procedure	es.
Assessment Methods And Objects		
settings and associated documentation; other re	cy; procedures addressing spam protection; information system design documentation; spam protection elevant documents or records.	mechanisms; information system configuration
Test: Spam detection and handling capability.		
SI-8(1) – Enhancement (High)		
Control		
Centrally manage spam protection mechanisms)	
Applicability: All	References: ARS: SI-8(1); HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8(1)	Related Controls:
ASSESSMENT PROCEDURE: SI-8(1).1		
Assessment Objective		
Determine if the organization centrally manages	s spam protection mechanisms.	
Assessment Methods And Objects		
Examine: System and information integrity police	cy; procedures addressing spam protection; information system design documentation; spam protection	mechanisms; information system configuration
settings and associated documentation; other re	elevant documents or records.	
SI-8(2) – Enhancement (High)		
Control		
Automatically update spam protection mechanis	sms.	
Applicability: All	References: ARS: SI-8(2); HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8(2)	Related Controls:
ASSESSMENT PROCEDURE: SI-8(2).1		
Assessment Objective		
Determine if the information system automatica	Ilv undates snam protection mechanisms	
Assessment Methods And Objects		
	cy; procedures addressing spam protection; information system design documentation; spam protection	mechanisms: information system configuration
settings and associated documentation; other re		
Test: Automatic update capability for spam prot		
SI-9 – Information Input Restrictions (H		
Control		aformation to the information system shall be
restricted beyond the typical access controls en	trict information input to the information system to authorized personnel. Personnel authorized to input in nployed by the system, including limitations based on specific operational / project responsibilities.	nformation to the information system shall be
Guidance		
Restrictions on personnel authorized to input in operational/project responsibilities.	formation to the information system may extend beyond the typical access controls employed by the system	tem and include limitations based on specific
Applicability: All	References: ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2,	Related Controls:
	5.6.2.5#2.1; NIST 800-53/53A: SI-9; PISP: 4.17.9	
Rev. 9	Page 199 of 207	BPSSM Appendix A. Attachment 1

ASSESSMENT PROCEDURE: SI-9.1		
Assessment Objective		
o	ility to input information to the information system to authorized personnel.	
Assessment Methods And Objects		
, , , , , , , , , , , , , , , , , , , ,	cy; procedures addressing information input restrictions; access control policy and procedures; separation	n of duties policy and procedures; information
	em configuration settings and associated documentation; other relevant documents or records.	
SI-10 – Information Accuracy, Complete	eness, Validity, and Authenticity (High)	
Control		
	for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.	
Guidance		
	d authenticity of information are accomplished as close to the point of origin as possible. Rules for check	
	ge, acceptable values) are in place to verify that inputs match specified definitions for format and content	
	inintentionally interpreted as commands. The extent to which the information system is able to check the	accuracy, completeness, validity, and
authenticity of information is guided by organiza Applicability: All	References: ARS: SI-10; FISCAM: TAN-3.1.1, TAY-1.2.1, TAY-1.4.1, TAY-2.1.3, TCP-2.1.2, TCP-	Related Controls:
Applicability. All	2.1.3, TCP-2.1.4; IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-10; PISP: 4.17.10	Related Controls.
ASSESSMENT PROCEDURE: SI-10.1		
Assessment Objective		
Determine if:		
	r accuracy, completeness, validity, and authenticity;	
	and authenticity of information is accomplished as close to the point of origin as possible;	
	ck the valid syntax of information inputs to verify that inputs match specified definitions for format and co	ntent: and
	on inputs passed to interpreters to prevent the content from being unintentionally interpreted as comman	
Assessment Methods And Objects		
	cy; procedures addressing information accuracy, completeness, validity, and authenticity; access control	policy and procedures; separation of duties
	ated tools and applications to verify accuracy, completeness, validity, and authenticity of information; info	
information system configuration settings and as	ssociated documentation; other relevant documents or records.	
Test: Information system capability for checking	information for accuracy, completeness, validity, and authenticity.	
SI-10(CMS-1) – Enhancement (High)		
Control		
Implement automated system checks of informa	tion for accuracy, completeness, validity, and authenticity.	
Applicability: All	References: ARS: SI-10(CMS-1); FISCAM: TAN-3.1.1, TCP-2.1.3, TCP-2.1.4; IRS-1075: 5.6.2.5#1.1-	Related Controls:
	2	
ASSESSMENT PROCEDURE: SI-10(CMS-1).	1	
Assessment Objective		
Determine if the information system checks info	rmation for accuracy, completeness, validity, and authenticity.	
Assessment Methods And Objects		
Examine: System and information integrity polic	cy; procedures addressing information accuracy, completeness, validity, and authenticity; access control	policy and procedures; separation of duties
	nated tools and applications to verify accuracy, completeness, validity, and authenticity of information; info	
, , , , , , , , , , , , , , , , , , , ,	ssociated documentation; other relevant documents or records to determine that automated system chec	ks of information for accuracy, completeness,
validity, and authenticity are performed.		determine the Participant of the State
, , , , , , , , , , , , , , , , , , ,	on integrity responsibilities to determine that automated system checks of information for accuracy, comp	neteness, validity, and authenticity are
performed.	mated system checks of information for accuracy, completeness, validity, and authenticity are performed	
SI-10(FIS-1) – Enhancement (High)	mater system enders or information for accuracy, completeness, valuaty, and authenticity are performed	
Control		una estidate Caldes de 🐨 👘 👘
I ne source document is well-designed to aid the	e preparer and facilitate data entry and includes document pre-numbering and preprinting of transaction t	ype and data field codes. The document
Rev 0	Page 200 of 207	BPSSM Appendix A Attachment 1

Applicability: All	References: FISCAM: TAN-1.1.1, TAN-1.1.2, TAN-1.1.3, TAY-1.1.1, TAY-1.1	1.2, TCP-1.2.1 Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-1).1		
Assessment Objective		
Determine if the organizational source docume	nt is well-designed to aid the preparer and facilitate data entry and includes docu ses and field codes are entered into the system to facilitate completeness and se	
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Blank document storage area.		
Examine: Procedures for recording and trackir	g of numbers if pre-numbered documents are used.	
Examine: Source documents and data entry ad	ctivities.	
Interview: User management and personnel.		
il-10(FIS-2) – Enhancement (High)		
Control		
For batch application systems, a batch control s identification of the user submitting the batch.	sheet is prepared for a group of source documents, and includes: date, control n	number, number of documents, a control total for a key field, and
Applicability: All; Optional for CWF, SS	References: FISCAM: TAN-1.1.4	Related Controls:
SSESSMENT PROCEDURE: SI-10(FIS-2).1		
ssessment Objective		
Determine if the organizational batch applicatio for a key field, and identification of the user sub Assessment Methods And Objects	n systems prepared a batch control sheet for a group of source documents, and mitting the batch.	includes: date, control number, number of documents, a control tota
Examine: Pertinent policies and procedures.		
	4°	
Examine: Datch control sheets if Datch applica	tion.	
Examine: Batch control sheets if batch applica Examine: Prepared source documents and bat		
Examine: Prepared source documents and bat	tches if batch application.	
Examine: Prepared source documents and bat Interview: Users responsible for preparing bate	tches if batch application.	
Examine: Prepared source documents and bat Interview: Users responsible for preparing bate SI-10(FIS-3) – Enhancement (High)	tches if batch application.	
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate II-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign	tches if batch application.	prepared and authorized; and monitor data entry and processing of
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate I-10(FIS-3) – Enhancement (High) ontrol Key source documents require authorizing sign source documents.	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p	prepared and authorized; and monitor data entry and processing of Related Controls:
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate II-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. pplicability: All; Optional for CWF, SS	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2	
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate SI-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. Applicability: All; Optional for CWF, SS ASSESSMENT PROCEDURE: SI-10(FIS-3).1	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2	
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate I-10(FIS-3) – Enhancement (High) Sontrol Key source documents require authorizing sign source documents. pplicability: All; Optional for CWF, SS ISSESSMENT PROCEDURE: SI-10(FIS-3).1 Issessment Objective	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so	Related Controls:
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate SI-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. SSESSMENT PROCEDURE: SI-10(FIS-3).1 SSESSMENT PROCEDURE: SI-10(FIS-3).1 SSESSMENT Objective Determine if the organizational key source docu data entry and processing of source documents	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so	Related Controls:
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate I-10(FIS-3) – Enhancement (High) Sontrol Key source documents require authorizing sign source documents. pplicability: All; Optional for CWF, SS ISSESSMENT PROCEDURE: SI-10(FIS-3).1 ISSESSMENT Objective Determine if the organizational key source docu data entry and processing of source documents	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s.	Related Controls:
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate I-10(FIS-3) – Enhancement (High) Sontrol Key source documents require authorizing sign source documents. pplicability: All; Optional for CWF, SS SSESSMENT PROCEDURE: SI-10(FIS-3).1 ISSESSMENT PROCEDURE: SI-10(FIS-3).1 ISSESSMENT Objective Determine if the organizational key source docu data entry and processing of source documents ISSESSMENT Methods And Objects Examine: Key source documents and data entry	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s. ry activities.	Related Controls:
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate I-10(FIS-3) – Enhancement (High) Sontrol Key source documents require authorizing sign source documents. pplicability: All; Optional for CWF, SS SSESSMENT PROCEDURE: SI-10(FIS-3).1 ISSESSMENT PROCEDURE: SI-10(FIS-3).1 ISSESSMENT Objective Determine if the organizational key source docu data entry and processing of source documents ISSESSMENT Methods And Objects Examine: Key source documents and data ent Examine: Pertinent policies and procedures. Interview: Management and data control unit p	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s. ry activities.	Related Controls:
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate I-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. pplicability: All; Optional for CWF, SS ISSESSMENT PROCEDURE: SI-10(FIS-3).1 ISSESSMENT PROCEDURE: SI-10(FIS-4).1 ISSESSMENT PROCEDURE:	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s. ry activities.	Related Controls:
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate SI-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. Spplicability: All; Optional for CWF, SS SSESSMENT PROCEDURE: SI-10(FIS-3).1 Assessment Objective Determine if the organizational key source docu data entry and processing of source documents Assessment Methods And Objects Examine: Key source documents and data ent Examine: Pertinent policies and procedures. Interview: Management and data control unit p SI-10(FIS-4) – Enhancement (High) Control	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s. ry activities. personnel.	Related Controls:
Examine: Prepared source documents and bal Interview: Users responsible for preparing bate I-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. pplicability: All; Optional for CWF, SS ISSESSMENT PROCEDURE: SI-10(FIS-3).1 ISSESSMENT PROCEDURE: SI-10(FIS-3).1 ISSESSMENT Objective Determine if the organizational key source docu data entry and processing of source documents ISSESSMENT Methods And Objects Examine: Key source documents and data entr Examine: Pertinent policies and procedures. Interview: Management and data control unit p Supervisory or control unit personnel review data	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s. ry activities. personnel. ta and enter an authorizing code before data is released for processing.	Related Controls:
Examine: Prepared source documents and bat Interview: Users responsible for preparing bate SI-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. Splicability: All; Optional for CWF, SS SSESSMENT PROCEDURE: SI-10(FIS-3).1 Assessment Objective Determine if the organizational key source docu data entry and processing of source documents Assessment Methods And Objects Examine: Key source documents and data ent Examine: Pertinent policies and procedures. Interview: Management and data control unit p Supervisory or control unit personnel review data Applicability: All	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s. ry activities. personnel. Ita and enter an authorizing code before data is released for processing. References: FISCAM: TAN-1.2.3	Related Controls:
Examine: Prepared source documents and bata Interview: Users responsible for preparing bata SI-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. Applicability: All; Optional for CWF, SS ASSESSMENT PROCEDURE: SI-10(FIS-3).1 Assessment Objective Determine if the organizational key source documents Assessment Methods And Objects Examine: Key source documents and data ent Examine: Pertinent policies and procedures. Interview: Management and data control unit p SI-10(FIS-4) – Enhancement (High) Control Supervisory or control unit personnel review da Applicability: All ASSESSMENT PROCEDURE: SI-10(FIS-4).1	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s. ry activities. personnel. Ita and enter an authorizing code before data is released for processing. References: FISCAM: TAN-1.2.3	Related Controls:
Examine: Prepared source documents and bat Interview: Users responsible for preparing bate SI-10(FIS-3) – Enhancement (High) Control Key source documents require authorizing sign source documents. Applicability: All; Optional for CWF, SS ASSESSMENT PROCEDURE: SI-10(FIS-3).1 Assessment Objective Determine if the organizational key source docu data entry and processing of source documents Assessment Methods And Objects Examine: Key source documents and data ent Examine: Pertinent policies and procedures. Interview: Management and data control unit p SI-10(FIS-4) – Enhancement (High) Control Supervisory or control unit personnel review da Applicability: All ASSESSMENT PROCEDURE: SI-10(FIS-4).1 Assessment Objective	tches if batch application. ch control sheets and submitting the batch. natures. Data control unit personnel: verify that source documents are properly p References: FISCAM: TAN-1.2.1, TAN-1.2.2 uments require authorizing signatures. Data control unit personnel: verify that so s. ry activities. personnel. Ita and enter an authorizing code before data is released for processing. References: FISCAM: TAN-1.2.3	Related Controls: ource documents are properly prepared and authorized; and monitor Related Controls:

Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Review process.	rooppol	
Interview: Management and data control unit per SI-10(FIS-5) – Enhancement (High)	rsonnei.	
Control		
	plication so that the action can be analyzed for appropriateness and correctness.	
Applicability: All; Optional for CWF	References: FISCAM: TAY-2.3.2	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-5).1	References. FIGGAM. TAT-2.3.2	Related Controls.
Assessment Objective		
	override is automatically logged by the application so that the action can be ana	lyzed for appropriateness and correctness
Assessment Methods And Objects	overhee is automatically logged by the application so that the action can be and	
Examine: Application documentation.		
Examine: Override audit logs.		
Interview: Application programmer, if available,	and user management personnel.	
SI-10(FIS-6) – Enhancement (High)		
Control		
	s are automatically assigned a unique sequence number, which is used by the co	omputer to monitor that all transactions are processed.
Applicability: All	References: FISCAM: TCP-1.2.2	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-6).1		
Assessment Objective		
•	m transactions without preassigned serial numbers are automatically assigned a	unique sequence number, which is used by the computer to monit
that all transactions are processed.	in ransactions without preassigned schar humbers are automatically assigned a	
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation generated	by system.	
Interview: Application programmer, if available.		
Interview: User management and personnel.		
SI-10(FIS-7) – Enhancement (High)		
Control		
Transactions are sequence checked and compu	ter matched with data in master or suspense files to identify missing or duplicate	transactions. Reports of missing or duplicate transactions are
produced, and items are investigated and resolv		
Applicability: All	References: FISCAM: TCP-1.2.3, TCP-1.2.4, TCP-1.3.1, TCP-1.3.2	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-7).1		
Assessment Objective		
Determine if the organizational information syste	m transactions are sequence checked and computer matched with data in maste	er or suspense files to identify missing or duplicate transactions.
	produced, and items are investigated and resolved in a timely manor.	
Assessment Methods And Objects		
Examine: Activity to investigate items reported a	as missing or duplicate.	
Examine: Application documentation.		
Examine: Pertinent policies and procedures.		
Examine: Reports of missing and duplicate tran	sactions.	
Interview: Application programmer, if available.		
Interview: User management and personnel.		
	D 202 (207	

SI 40/FIS 9) Enhancement (Lisch)			
SI-10(FIS-8) – Enhancement (High)			
Control	and the second		and the second state of th
	compared with a detailed listing of items processed by the computer, partic	ularly to control important lov	
Applicability: All; Optional for CWF	References: FISCAM: TCP-1.4.1		Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-8).1			
Assessment Objective	n la individual transportione ar course desumente are compored with a datail	lad liating of itama processo	by the computer perticularly to control
important low-volume, high-value transactions.	em's individual transactions or source documents are compared with a detail	ed listing of items processed	by the computer, particularly to control
Assessment Methods And Objects			
Examine: Comparison activity.			
Examine: Listings for notations showing checking	ng was performed.		
Examine: Pertinent policies and procedures.			
Interview: User management and personnel.			
SI-11 – Error Handling (High)			
Control			
	ror conditions in an expeditious manner. User error messages generated by bited by adversaries. System error messages shall be revealed only to author		
Guidance			
system provide timely and useful information wit	e carefully considered by the organization. Error messages are revealed only thout revealing potentially harmful information that could be used by adversa d in error logs or associated administrative messages. The extent to which th	aries. Sensitive information (e	e.g., account numbers, social security
guided by organizational policy and operational i		le information system is able	
Applicability: All	References: ARS: SI-11; FISCAM: TAY-3.2.1; NIST 800-53/53A: SI-11; P	ISP: 4.17.11	Related Controls: SI-2
ASSESSMENT PROCEDURE: SI-11.1			
Assessment Objective			
Determine if:			
	error conditions in an expeditious manner without providing information that	could be exploited by adve	saries;
(ii) the information system reveals only essential	l information to authorized individuals; and		
(iii) the information system does not include sense	sitive information in error logs or associated administrative messages.		
Assessment Methods And Objects			
Examine: System and information integrity polic associated documentation; other relevant docum	cy; procedures addressing information system error handling; information system error handling; information sys	stem design documentation;	information system configuration settings and
Test: Information system error handling capabili			
SI-11(0) – Enhancement (High)			
Control			
	rror messages providing timely and useful information to users without revea	aling information that could k	e exploited by adversaries Ensure
	User IDs, social security numbers, etc.) is not listed in error logs or associat		
Applicability: All	References: ARS: SI-11(0); FISCAM: TAY-4.1.8; NIST 800-53/53A: SI-11		Related Controls:
ASSESSMENT PROCEDURE: SI-11(0).1		, , , , , , , , , , , , , , , , , , , ,	
Assessment Objective			
		s as prescribed in this amplif	ving anhoncoment to the baseline control
	nents as specified in the baseline control and the specific CMS requirements		VING ENNANCEMENT TO THE DASENNE CONTOL
o 1	nents as specified in the baseline control and the specific CMS requirements	s as prescribed in this ampli	ying enhancement to the baseline control.
Assessment Methods And Objects	cy; procedures addressing information system error handling; information error handling;		

SI-11(FIS-1) – Enhancement (High)	
Control	
Rejected data are automatically written on an automated error suspense file and purged as corrected. Each erroneous transaction is annotated with: (1)	codes indicating the type of data error (2)
date and time the transaction was processed and the error identified, and (3) the identity of the user who originated the transaction. Record counts and c	
suspense file and used in reconciling transactions processed.	
Applicability: All References: FISCAM: TAY-3.1.1, TAY-3.1.2, TAY-3.1.4	Related Controls:
ASSESSMENT PROCEDURE: SI-11(FIS-1).1	
Assessment Objective	
Determine if the organizational information system's rejected data is automatically written on an automated error suspense file and purged as corrected.	Each erroneous transaction is annotated with:
(1) codes indicating the type of data error, (2) date and time the transaction was processed and the error identified, and (3) the identity of the user who or	
control totals are established over the suspense file and used in reconciling transactions processed.	-
Assessment Methods And Objects	
Examine: Application documentation and interview application programmers, if available.	
Examine: Reports produced from the suspense file.	
Interview: User management and personnel.	
Test: Verify process with test transactions containing errors.	
SI-11(FIS-2) – Enhancement (High)	
Control	
A control group is responsible for: reviewing suspense file control total reports, determining completeness of processing, and controlling and monitoring r	ejected transactions
Applicability: All; Optional for CWF, SS References: FISCAM: TAY-3.1.3	Related Controls:
ASSESSMENT PROCEDURE: SI-11(FIS-2).1	
Assessment Objective	
Determine if the organizational information system's control group is responsible for: reviewing suspense file control total reports, determining completen-	ess of processing, and controlling and
monitoring rejected transactions	
Assessment Methods And Objects	
Examine: Pertinent policies and procedures.	
Examine: Reports produced from the suspense file.	
Interview: User management and control group.	
Test: Verify review process with test transactions containing errors.	
SI-11(FIS-3) – Enhancement (High)	
Control	
The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age	of uncorrected transactions.
Applicability: All; Optional for CWF, DC, EDC, SS References: FISCAM: TAY-3.1.5	Related Controls:
ASSESSMENT PROCEDURE: SI-11(FIS-3).1	
Assessment Objective	
Determine if:	
(i) the organizational information system [The suspense file] is produced, on a regular basis for management review; and	
(ii) the organization determines the level and type of transaction errors and the age of uncorrected transactions.	
Assessment Methods And Objects	
Examine: Analysis reports produced from the suspense file.	
Examine: Application documentation.	
Examine: Pertinent policies and procedures.	
Interview: User management and control group.	
SI-11(FIS-4) – Enhancement (High)	
Control	
Errors are corrected by the user originating the transaction, and all corrections are reviewed and approved by supervisors before the corrections are reer	ntered.

Applicability: All	References: FISCAM: TAY-3.2.2, TAY-3.2.3	Related Controls:
ASSESSMENT PROCEDUR	E: SI-11(FIS-4).1	
Assessment Objective		
5	al information system errors are corrected by the user originating the	e transaction, and all corrections are reviewed and approved by supervisors before the corrections ar
reentered.		
Assessment Methods And	-	
Examine: Error correction a	ctivities.	
Examine: Error reports.		
Examine: Pertinent policies	•	
Interview: User manageme	•	
Test: Verify test transaction SI-11(FIS-5) – Enhancemen		
Control		
	le for: reviewing control total reports, determining completeness of pro	accessing, and controlling and monitoring rejected transactions
Applicability: All; Optional for S		Related Controls:
ASSESSMENT PROCEDUR		Related Controls.
	31-11(F13-3).1	
Assessment Objective	and control group is reasonable for reviewing control total reports do	termining completeness of processing and controlling and manitaring rejected transactions
-		termining completeness of processing, and controlling and monitoring rejected transactions
Assessment Methods And	•	
Examine: Application docu		
Examine: Pertinent policies		
	oleteness of processing activities.	
Interview: Data control per		
Interview: User manageme		
	ut Handling and Retention (High)	
Control		
	ems shall be handled and retained in accordance with applicable laws	vs, Executive Orders, directives, policies, regulations, standards, operational requirements, and the
information sensitivity level.		
Guidance		
o i i	edures for handling sensitive output information is the NIST SP.	
Applicability: All	References: ARS: SI-12; FISCAM: TAY-4.1.6; T 53/53A: SI-12; PISP: 4.17.12	IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2; NIST 800- Related Controls:
ASSESSMENT PROCEDUR		
Assessment Objective	01-12.1	
Determine if:		
	and retains output from the information system in accordance with an	plicable laws, Executive Orders, directives, policies, regulations, standards, and operational
requirements; and		plicable laws, Executive Orders, directives, policies, regulations, standards, and operational
	output from the information system in accordance with labeled or may	rked instructions on information system output (including paper and digital media) that includes, but
	tions for dissemination, distribution, transport, or storage of information	
Assessment Methods And		
	•	tput handling and retention; media protection policy and procedures; information retention records,
other relevant documents o		
		25
	rsonnel with information output handling and retention responsibilitie.	
SI-12(CMS-1) – Enhanceme	ersonnel with information output handling and retention responsibilities nt (High)	
SI-12(CMS-1) – Enhanceme Control		
Control	nt (High)	
Control Retain output, including, bu	nt (High)	eports, and business records, from the information system in accordance with CMS Policy and all

Applicability: All	References: ARS: SI-12(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2	Related Controls:
ASSESSMENT PROCEDURE: SI-12(CM		
Assessment Objective		
	but, including, but not limited to audit records, system reports, business and financial reports, and	d business records, from the information system in
accordance with CMS Policy and all appli		
Assessment Methods And Objects		
Examine: At a minimum, documentation	for record retention of audit records, system reports, business and financial reports, and busine	ess records are in accordance with CMS Policy and all
applicable NARA requirements.		
SI-12(FIS-1) – Enhancement (High)		
Control		
	all outputs are produced and distributed according to system requirements and design by a dat	
	dule by application that shows when outputs should be completed, when they need to be distributed by application that shows when outputs should be completed.	uted, who the recipients are, and the copies needed; (2)
	ptability; and (3) reconciles control information to determine completeness of processing.	Deleted Controles
	References: FISCAM: TAY-4.1.1, TAY-4.1.2	Related Controls:
ASSESSMENT PROCEDURE: SI-12(FIS	5-1).1	
Assessment Objective		
	sponsibility for seeing that all outputs are produced and distributed according to system requirem	
	pup: (1) has a schedule by application that shows when outputs should be completed, when they general acceptability; and (3) reconciles control information to determine completeness of process	
Assessment Methods And Objects		song.
Examine: Output production and distribu	ition	
Examine: Pertinent policies and procedu		
Interview: Information system and user r		
SI-12(FIS-2) – Enhancement (High)		
Control	eport name, time and date of production, the processing period covered; and have an "end-of-re	eport" message.
Control	eport name, time and date of production, the processing period covered; and have an "end-of-re References: FISCAM: TAY-4.1.3	eport" message. Related Controls:
Control Printed reports contain a title page with re	References: FISCAM: TAY-4.1.3	
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS	References: FISCAM: TAY-4.1.3	
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective	References: FISCAM: TAY-4.1.3 S-2).1	Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective	References: FISCAM: TAY-4.1.3	Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects	References: FISCAM: TAY-4.1.3 S-2).1	Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation.	References: FISCAM: TAY-4.1.3 S-2).1	Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports.	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the	Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and application	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the	Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports.	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the	Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and application	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the	Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and applicatio SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed o	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the report	Related Controls: processing period covered; and have an "end-of-report" ecipient(s) who receive the output.
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and application SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed of Applicability: All	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the references: FISCAM: TAY-4.1.4, TAY-4.1.5	Related Controls: processing period covered; and have an "end-of-report"
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and applicatio SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed o	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the references: FISCAM: TAY-4.1.4, TAY-4.1.5	Related Controls: processing period covered; and have an "end-of-report" ecipient(s) who receive the output.
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational information message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and application SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed of Applicability: All	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the references: FISCAM: TAY-4.1.4, TAY-4.1.5	Related Controls: processing period covered; and have an "end-of-report" ecipient(s) who receive the output.
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and applicatio SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed o Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the references: FISCAM: TAY-4.1.4, TAY-4.1.5	Related Controls: processing period covered; and have an "end-of-report" ecipient(s) who receive the output. Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio message. Assessment Methods And Objects Examine: Printed reports. Interview: User personnel and applicatio SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed o Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio	References: FISCAM: TAY-4.1.3 S-2).1 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the re References: FISCAM: TAY-4.1.4, TAY-4.1.5 S-3).1	Related Controls: processing period covered; and have an "end-of-report" ecipient(s) who receive the output. Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and applicatio SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed o Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio receive the output. Assessment Methods And Objects Examine: Application documentation.	References: FISCAM: TAY-4.1.3 S-2).1 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the re References: FISCAM: TAY-4.1.4, TAY-4.1.5 S-3).1	Related Controls: processing period covered; and have an "end-of-report" ecipient(s) who receive the output. Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and applicatio SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed o Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio receive the output. Assessment Methods And Objects Examine: Application documentation. Examine: Output logs.	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the regime references: FISCAM: TAY-4.1.4, TAY-4.1.5 S-3).1 on system's output produced, whether printed or transmitted to a user's terminal device, is logged	Related Controls: processing period covered; and have an "end-of-report" ecipient(s) who receive the output. Related Controls:
Control Printed reports contain a title page with re Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio message. Assessment Methods And Objects Examine: Application documentation. Examine: Printed reports. Interview: User personnel and applicatio SI-12(FIS-3) – Enhancement (High) Control Each output produced, whether printed o Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS Assessment Objective Determine if the organizational informatio receive the output. Assessment Methods And Objects Examine: Application documentation.	References: FISCAM: TAY-4.1.3 S-2).1 on system printed reports contain a title page with report name, time and date of production, the on programmer, if available. or transmitted to a user's terminal device, is logged, manually if not automatically, including the regime references: FISCAM: TAY-4.1.4, TAY-4.1.5 S-3).1 on system's output produced, whether printed or transmitted to a user's terminal device, is logged	Related Controls: processing period covered; and have an "end-of-report" ecipient(s) who receive the output. Related Controls:

SI-12(FIS-4) – Enhancemer	ht (High)	
Control		
	tputs transmitted are summarized daily and printed for each terminal device, and reviewed by	supervisors. A control log of output product errors is maintained, including the
corrective actions take.		
Applicability: All	References: FISCAM: TAY-4.1.7, TAY-4.1.8	Related Controls:
ASSESSMENT PROCEDUR	{E: SI-12(FIS-4).1	
Assessment Objective		
	onal information system's user department, outputs transmitted are summarized daily and prir aintained, including the corrective actions take.	nted for each terminal device, and reviewed by supervisors. A control log of
Assessment Methods And	Objects	
Examine: Pertinent policie	s and procedures.	
Examine: Supporting docu	mentation (e.g., printed daily summaries with supervisory initials or signatures).	
Examine: This activity.		
Interview: User supervisor		
SI-12(FIS-5) – Enhancemer	ht (High)	
Control		
	s for data accuracy, validity, and completeness. The reports include: (1) error reports, (2) tran- eports. Output from reruns is subjected to the same quality review as the original output.	saction reports, (3) master record change reports, (4) exception reports, and
Applicability: All	References: FISCAM: TAY-4.1.9, TAY-4.2.1	Related Controls:
ASSESSMENT PROCEDUR	₹E: SI-12(FIS-5).1	
Assessment Objective		
-	onal users review output reports for data accuracy, validity, and completeness. The reports in	clude: (1) error reports, (2) transaction reports, (3) master record change
	rts, and (5) control totals balance reports. Output from reruns is subjected to the same quality	
Assessment Methods And	Objects	
Examine: Activity to review	v output reports.	
,		
Examine: Output reports.		

Business Partners Systems Security Manual

Appendix A, Attachment 2

CMS Core Security Requirements (CSR)

for

Moderate Impact Level Assessments



CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

Rev. 9

(This page intentionally left blank)

Access Control (AC) – Technical

AC-1 – Access Control Policy and Procedures (Moderate)

Control

Logical access controls and procedures shall be established and implemented effectively to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (i.e., programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

Guidance

The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

References: ARS: AC-1; FISCAM: TAC-3.2.C.1, TAC-4.3.4, TSD-1.1.1, TSD-2.1, TSS-1.1.1; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1; NIST 800-53/53A: AC-1; PISP: 4.1.1	Related Controls:

ASSESSMENT PROCEDURE: AC-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents access control policy and procedures;

(ii) the organization disseminates access control policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review access control policy and procedures; and

(iv) the organization updates access control policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities.(Optional)

ASSESSMENT PROCEDURE: AC-1.2

Assessment Objective

Determine if:

(i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities.(Optional)

AC-1(FIS-1) – Enhancement (Moderate)

Control

Standard forms are used to document approval for archiving, deleting, or sharing data files. Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

Applicability: All	References: FISCAM: TAC-2.3.1, TAC-2.3.2	Related Controls:
ASSESSMENT PROCEDURE: AC-1(FIS-1).1		

Assessment Objective

Determine if:

(i) the organization uses standard forms to document approval for archiving, deleting, or sharing data files; and

(ii) the organizational agreements, with other entities, document prior to sharing data or programs how the data files are protected.

Assessment Methods And Objects

Examine: Documents authorizing file sharing and file sharing agreements.

Examine: Pertinent policies and procedures.

Examine: Standard approval forms.

Interview: Data owners.

AC-2 – Account Management (Moderate)

Control

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. Access to the CMS information system shall be granted based on: (a) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (b) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

Guidance

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system usage or need-to-know/need-to-share changes.

Applicability: All	References: ARS: AC-2; FISCAM: TAC-3.2.C.4, TAC-3.2.C.5, TSP-4.1.6, TSS-1.1.3; HIPAA:	Related Controls:
	164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1; NIST 800-	
	53/53A: AC-2; PISP: 4.1.2	
ACCECOMENT DROOFDURE: AC A4	•	

ASSESSMENT PROCEDURE: AC-2.1

Assessment Objective

Determine if:

(i) the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts;

(ii) the organization defines the frequency of information system account reviews;

(iii) the organization reviews information system accounts at the organization-defined frequency, at least annually; and

(iv) the organization initiates required actions on information system accounts based on the review.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing account management; information system security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities.

interview. Organizational person		
AC-2(0) – Enhancement (Moder	ate)	
Control		
Review information system acco	unts every 180 days and require annual certification.	
Applicability: All	References: ARS: AC-2(0); FISCAM: TAC-3.2.C.4, TSS-1.1.4; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2	Related Controls:
ASSESSMENT PROCEDURE: A	C-2(0).1	
Assessment Objective		
Determine if the organization me	ets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this ar	nplifying enhancement to the baseline control.
Assessment Methods And Obje	ects	
	account management procedures; information system security plan (for organization-defined account review freque ed employees; list of recently disabled information system accounts; system-generated records with user IDs and la	

records.

Interview: Organizational personnel with account management responsibilities.

AC-2(1) – Enhancement (Moderate)		
Control		
Employ automated mechanisms to support the r	nanagement of information system accounts.	
Applicability: All	References: ARS: AC-2(1); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(1)	Related Controls:

ASSESSMENT PROCEDURE: AC-2(1).1		
Assessment Objective		
	d mechanisms to support information system account management functions.	
Assessment Methods And Objects	a mechanisms to support information system account management functions.	
	gement; information system design documentation; information system configuration settings and asso	ociated documentation: other relevant
documents or records.		
Test: Automated mechanisms implementing acc	ount management functions (Ontional)	
AC-2(2) – Enhancement (Moderate)		
Control	ensurement for a marined of time NITE 0.4 hours and to allow accounts with a fixed dynation (i.e. to an	
	ency account for a period of time NTE 24 hours and to allow accounts with a fixed duration (i.e., tempo	
	References: ARS: AC-2(2); FISCAM: TAC-2.2; IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(2)	Related Controls:
ASSESSMENT PROCEDURE: AC-2(2).1		
Assessment Objective		
Determine if:		
() U	ich the information system terminates temporary and emergency accounts; and	
	es temporary and emergency accounts after organization-defined time period for each type of account	
Assessment Methods And Objects		
	mation system design documentation; information system configuration settings and associated docun	nentation; information system audit records;
other relevant documents or records.	ourt monogement functions (Ontional)	
Test: Automated mechanisms implementing acc	ount management functions.(Optional)	
AC-2(3) – Enhancement (Moderate)		
Control		
Configure the information system to disable inac		
Applicability: All	References: ARS: AC-2(3); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(3	3) Related Controls: IA-4(0)
ASSESSMENT PROCEDURE: AC-2(3).1		
Assessment Objective		
Determine if:		
(i) the organization defines a time period after who	ich the information system disables inactive accounts; and	
	inactive accounts after organization-defined time period.	
Assessment Methods And Objects		
	gement; information system security plan; information system design documentation; information syste	
	t of last login dates; information system-generated list of active accounts; information system audit rec	ords; other relevant documents or records.
Test: Automated mechanisms implementing acc	ount management functions.(Optional)	
AC-2(4) – Enhancement (Moderate)		
Control		
Employ automated mechanisms to audit user ac	count creation, modification, disabling, and termination. Ensure the automated mechanism notifies app	propriate personnel of the user account
management actions.		
Applicability: All	References: ARS: AC-2(4); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2(4)	Related Controls:
ASSESSMENT PROCEDURE: AC-2(4).1		
Assessment Objective		
Determine if:		
(i) the organization employs automated mechani	sms to audit account creation, modification, disabling, and termination actions; and	
(ii) the organization employs automated mechan	sms to notify, as required, appropriate individuals.	
Assessment Methods And Objects		
Examine: Procedures addressing account mana	gement; information system design documentation; information system configuration settings and asso	ociated documentation; information system
audit records; other relevant documents or recor		-
Test: Automated mechanisms implementing acc	ount management functions.(Optional)	
Rev. 9	Page 3 of 189	BPSSM Appendix A, Attachment 2
	C	11 /

AC-2(CMS-1) – Enhancement (Modera		
	ate)	
Control		
Remove or disable default user account		
Applicability: All	References: ARS: AC-2(CMS-1); FISCAM: TAC-3.2.A.3, TAC-3.2.C.4, TSS-1.2.3; IRS-1075 5.6.3.2#2.1	E Related Controls:
ASSESSMENT PROCEDURE: AC-2(CI	MS-1).1	
Assessment Objective		
Determine if the organization manages i	information system accounts, including establishing, activating, modifying, reviewing, disabling, and rer	moving accounts.
Assessment Methods And Objects		
Examine: Access control policy and pro accounts if they must be used.	ocedures; other relevant documents or records to determine if the organization removes or disables def	fault user accounts. It must also rename active default
renamed.	h access control responsibilities to determine that all default user accounts are either removed or disat	
Test: Information system sample of hos	ts with defined users to ensure that all default user accounts are either removed or disabled. If default	accounts are active, that they are renamed.
AC-2(CMS-2) - Enhancement (Modera	ate)	
Control		
Require the use of unique and separate	administrator accounts for administrator and non-administrator activities.	
Applicability: All	References: ARS: AC-2(CMS-2); FISCAM: TAN-2.1.4; IRS-1075: 5.6.3.2#2.1	Related Controls: IA-4(CMS-1)
ASSESSMENT PROCEDURE: AC-2(CI	MS-2).1	
Assessment Objective	· · · ·	
	orces separation of duties through assigned access authorizations.	
Assessment Methods And Objects		
of recently separated or terminated emp	nt management procedures; information system security plan (for organization-defined account review ployees; list of recently disabled information system accounts; system-generated records with user IDs s administrator accounts to be used for day-to-day activities.	
0 1	h account management responsibilities to determine if administrator accounts are being used for day to	
Test: Information system sample of hos	the sector of the sector of the sector description and the sector of the	o day activities.
AC-2(CMS-3) – Enhancement (Modera	ts' system logs to ensure that administrator accounts are not being used for day-to-day activities.	o day activities.
AC-2(CMS-5) - Emiancement (Modera		o day activities.
Control		o day activities.
	ate)	o day activities.
Control Implement centralized control of user ac	ate)	
Control Implement centralized control of user ac Applicability: All	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1	o day activities. Related Controls:
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(Cl	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1	·
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(CI Assessment Objective	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1	Related Controls:
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(Cl Assessment Objective Determine if the organization manages i	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1 MS-3).1	Related Controls:
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(Cl Assessment Objective Determine if the organization manages i Assessment Methods And Objects Examine: Access control policy; account	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1 MS-3).1 information system accounts, including establishing, activating, modifying, reviewing, disabling, and rement management procedures; information system security plan (for organization-defined account review)	Related Controls: moving accounts. frequency); list of active user and system accounts; list
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(Cl Assessment Objective Determine if the organization manages i Assessment Methods And Objects Examine: Access control policy; account	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1 MS-3).1 information system accounts, including establishing, activating, modifying, reviewing, disabling, and rement procedures; information system security plan (for organization-defined account review ployees; list of recently disabled information system accounts; system-generated records with user IDs	Related Controls: moving accounts. frequency); list of active user and system accounts; list
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(Cl Assessment Objective Determine if the organization manages i Assessment Methods And Objects Examine: Access control policy; accoun of recently separated or terminated emp to determine if all user access administra Interview: Organizational personnel with	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1 MS-3).1 information system accounts, including establishing, activating, modifying, reviewing, disabling, and rement procedures; information system security plan (for organization-defined account review ployees; list of recently disabled information system accounts; system-generated records with user IDs ator functions are centralized. h account management responsibilities to determine if all user access administrator functions are carri	Related Controls: moving accounts. frequency); list of active user and system accounts; list and last login date; other relevant documents or records ed out by a centralized administrator function.
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(Cl Assessment Objective Determine if the organization manages i Assessment Methods And Objects Examine: Access control policy; accoun of recently separated or terminated emp to determine if all user access administra Interview: Organizational personnel with	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1 MS-3).1 information system accounts, including establishing, activating, modifying, reviewing, disabling, and rement procedures; information system security plan (for organization-defined account review ployees; list of recently disabled information system accounts; system-generated records with user IDs rator functions are centralized.	Related Controls: moving accounts. frequency); list of active user and system accounts; list and last login date; other relevant documents or records ed out by a centralized administrator function.
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(Cl Assessment Objective Determine if the organization manages i Assessment Methods And Objects Examine: Access control policy; accoun of recently separated or terminated emp to determine if all user access administra Interview: Organizational personnel with	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1 MS-3).1 information system accounts, including establishing, activating, modifying, reviewing, disabling, and rement procedures; information system security plan (for organization-defined account review ployees; list of recently disabled information system accounts; system-generated records with user IDs ator functions are centralized. h account management responsibilities to determine if all user access administrator functions are carried out by a centralized account functis account functions are carried out by a centralized a	Related Controls: moving accounts. frequency); list of active user and system accounts; list and last login date; other relevant documents or records ed out by a centralized administrator function.
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(CI Assessment Objective Determine if the organization manages i Assessment Methods And Objects Examine: Access control policy; accoun of recently separated or terminated emp to determine if all user access administra Interview: Organizational personnel with Test: Information system sample of host	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1 MS-3).1 information system accounts, including establishing, activating, modifying, reviewing, disabling, and rement procedures; information system security plan (for organization-defined account review ployees; list of recently disabled information system accounts; system-generated records with user IDs ator functions are centralized. h account management responsibilities to determine if all user access administrator functions are carried out by a centralized account functis account functions are carried out by a centralized a	Related Controls: moving accounts. frequency); list of active user and system accounts; list and last login date; other relevant documents or records ed out by a centralized administrator function.
Control Implement centralized control of user ac Applicability: All ASSESSMENT PROCEDURE: AC-2(CI Assessment Objective Determine if the organization manages i Assessment Methods And Objects Examine: Access control policy; account of recently separated or terminated emp to determine if all user access administra Interview: Organizational personnel with Test: Information system sample of host AC-2(CMS-4) – Enhancement (Modera Control	ate) ccess administrator functions. References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1 MS-3).1 information system accounts, including establishing, activating, modifying, reviewing, disabling, and rement procedures; information system security plan (for organization-defined account review ployees; list of recently disabled information system accounts; system-generated records with user IDs ator functions are centralized. h account management responsibilities to determine if all user access administrator functions are carried out by a centralized account functis account functions are carried out by a centralized a	Related Controls: moving accounts. frequency); list of active user and system accounts; list and last login date; other relevant documents or records ed out by a centralized administrator function.

ASSESSMENT PROCEDURE: AC-2(CMS-4).1 **Assessment Objective** Determine if the organization documents contractor security requirements and maintains contractor access privileges. **Assessment Methods And Objects** Examine: Access control policy; account management procedures; information system security plan (for organization-defined account review frequency); list of active user and system accounts; list of recently separated or terminated employees; list of recently disabled information system accounts; system-generated records with user IDs and last login date; other relevant documents or records to determine if all contractors' access are authorized, regulated, and security requirements for contractors are defined. Interview: Organizational personnel with account management responsibilities to determine if written authorizations exist for a sample of contractor employees. AC-2(CMS-5) – Enhancement (Moderate) Control Revoke employee access rights upon termination. Physical access must be revoked immediately following employee termination, and system access must be revoked prior to or during the termination process. Applicability: All References: ARS: AC-2(CMS-5); FISCAM: TSP-4.1.6; IRS-1075: 5.6.3.2#2.1 **Related Controls:** ASSESSMENT PROCEDURE: AC-2(CMS-5).1 **Assessment Objective** Determine if the organization terminates information system access upon termination of individual employment. **Assessment Methods And Objects** Examine: Access control policy; account management procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine when employee access rights are revoked on termination. Interview: Organizational personnel with personnel security responsibilities to determine when access is revoked on employee termination. AC-2(FIS-1) – Enhancement (Moderate) Control All system access authorizations are: (1) documented on standard forms and maintained on file, (2) approved by senior managers, and (3) securely transferred to security managers. Guidance The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties. Applicability: All References: FISCAM: TAC-2.1.1. TAC-2.2 **Related Controls:** ASSESSMENT PROCEDURE: AC-2(FIS-1).1 **Assessment Objective** Determine if: (i) the organization grants system access authorizations on standard forms and maintains the completed forms on file; and (ii) the organizational senior managers approve system access authorizations and the approvals are securely transferred to security managers. **Assessment Methods And Objects** Examine: Pertinent policies and procedures. Examine: Selection of user (both application user and information system personnel) access authorization documentation. Interview: Personnel involved in access authorizations and senior managers who approve authorizations. AC-2(FIS-2) – Enhancement (Moderate) Control Business Owners periodically review system access authorization listings and determine whether they remain appropriate. ISSO/SSOs review system access authorizations and discuss any questionable authorizations with Business Owners. Applicability: All References: FISCAM: TAC-2.1.2, TAC-2.1.4 **Related Controls:** ASSESSMENT PROCEDURE: AC-2(FIS-2).1 **Assessment Objective** Determine if the organization ISSO/SSOs periodically reviews system access authorization listings and discusses guestionable authorizations with management. **Assessment Methods And Objects**

Examine: Access authorization listings to determine whether inappropriate access are removed in a timely manner.

Examine: Pertinent policies and procedures.		1
	ing documentation. Determine whether inappropriate access is removed in a timely manner.	
Interview: ISSO/SSOs and review documentation	n provided to them.	
AC-3 – Access Enforcement (Moderate)		
Control		
in a CMS information system. Additional applica	oped, documented and implemented effectively to control access between named users (or processes) a tion level access enforcement mechanism shall be implemented, when necessary, to provide increased ed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (s	information security for CMS information.
Guidance		
Access control policies (e.g., identity-based polic cryptography) are employed by organizations to information system. In addition to controlling acc information security for the organization. Conside serious events. If encryption of stored information	ies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., acc control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, ru ess at the information system level, access enforcement mechanisms are employed at the application le eration is given to the implementation of a controlled, audited, and manual override of automated mechan n is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended	ecords, processes, programs, domains) in the vel, when necessary, to provide increased hisms in the event of emergencies or other d) compliant.
Applicability: All	References: ARS: AC-3; FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.C.6, TAC-3.2.D.1, TCC-3.2.3, TSS-2.1.1, TSS-2.1.2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3; NIST 800-53/53A: AC-3; PISP: 4.1.3	Related Controls: MA-CMS-1, MA-CMS-2, SC-13
ASSESSMENT PROCEDURE: AC-3.1		
 (ii) user privileges on the information system are Assessment Methods And Objects Examine: Access control policy; procedures add privileges); information system audit records; oth Test: Automated mechanisms implementing acc AC-3(1) – Enhancement (Moderate) Control Ensure the information system restricts access to relevant information is restricted to explicitly authorized personnel include, for examinement 	ess enforcement policy.(Optional) o privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardw	vare, software, and firmware; and security
Applicability: All	References: ARS: AC-3(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.2, TAC-3.2.C.5, TAC-3.2.D.1, TCC- 3.2.3, TSD-3.1.4, TSS-1.1.2, TSS-2.1.2; IRS-1075: 5.6.3.2#2.2; NIST 800-53/53A: AC-3(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-3(1).1		
 (ii) the organization explicitly authorizes personner, (iii) the information system restricts access to privadministrators). Assessment Methods And Objects Examine: Access control policy; procedures additional system is a straight of the system is a straight	nctions and security-relevant information for the information system; el access to privileged functions and security-relevant information in accordance with organizational polic vileged functions (deployed in hardware, software, and firmware) and security-relevant information to exp lressing access enforcement; list of privileged functions and security relevant information; information system	licitly authorized personnel (e.g., security
Test: Automated mechanisms implementing acc		

AC-3(CMS-1) – Enhancement (Moderate)

Control

If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Applicability: All	References: ARS: AC-3(CMS-1); IRS-1075: 5.6.3.2#2.2	Related Controls: SC-13
ASSESSMENT PROCEDURE: AC-3(CMS-1).		

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if encryption is used as an access control mechanism, examine system and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Interview: Organizational personnel with access control responsibilities to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Test: Information system if encryption is used as an access control mechanism; examine organization's encryption key lengths, algorithms, certificates, etc.

AC-3(CMS-2) – Enhancement (Moderate)

Control

If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix A for e-Authentication Standards.

Applicability: All	References: ARS: AC-3(CMS-2); IRS-1075: 5.6.3.2#2.2	Related Controls:
ASSESSMENT PROCEDURE: AC-3(CMS-2).	1	

Assessment Objective

Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if e-authentication is used as an access control mechanism, examine Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the organization's encryption standard meets ARS Appendix A for e-Authentication Standards.

Interview: Organizational personnel with access control responsibilities if e-authentication is used as an access control mechanism, interview system administrators responsible for the hosts providing authentication services to determine if the organization meets the standards described in ARS Appendix A.

Test: Information system if e-authentication is used as an access control mechanism; test a sample of hosts for automated mechanisms implementing identification and authentication capability for the information system.

AC-3(CMS-3) – Enhancement (Moderate)

Control

Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information.

Applicability: All	References: ARS: AC-3(CMS-3); FISCAM: TAC-3.2.D.1, TCC-3.2.3; IRS-1075: 5.6.2.3#1, 5.6.3.2#2.2	Related Controls:

ASSESSMENT PROCEDURE: AC-3(CMS-3).1

Assessment Objective

Determine if the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive

information.

Interview: Organizational personnel with access control responsibilities to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

Test: Automated mechanisms implementing access enforcement policy to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

AC-3(CMS-4) – Enhancement (Moderate)

Control

Data stored in the information system must be protected with system access controls.

Applicability: All	References: ARS: AC-3(CMS-4); FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.D.1, TAY-3.1.6,	Related Controls:
	TCC-3.2.3; HIPAA: 164.312(a)(2)(iv); IRS-1075: 5.6.3.2#2.2	

ASSESSMENT PROCEDURE: AC-3(CMS-4).1

Assessment Objective

Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records to determine if data stored in the information system is protected with system access controls and must be encrypted when residing in non-secure areas.

Interview: Organizational personnel with access control responsibilities to determine if hosts storing data are protected with system access controls and if data stored in non-secure areas are encrypted.

Test: Automated mechanisms implementing access enforcement policy to if data stored on these hosts is protected with system access controls and that it is encrypted if residing in non-secure areas.

AC-4 – Information Flow Enforcement (Moderate)

Control

Flow control shall be enforced over information between source and destination objects within CMS information systems and between interconnected systems based on the characteristics of the information.

Guidance

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

Applicability: All	References: ARS: AC-4; IRS-1075: 5.6.3.2#2.2; NIST 800-53/53A: AC-4; PISP: 4.1.4	Related Controls: SC-7
ASSESSMENT PROCEDURE: AC-4.1		

Assessment Objective

Determine if the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records. Test: Automated mechanisms implementing information flow enforcement policy.(Optional)

ASSESSMENT PROCEDURE: AC-4.2

Assessment Objective

Determine if interconnection agreements address the types of permissible and impermissible flow of information between information systems and the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information flow enforcement; information system interconnection agreements; information system configuration settings and associated

documentation; list of information flow control authorizations; information system audit records; other relevant documents or records.

AC-5 – Separation of Duties (Moderate)

Control

The principle of separation of duties shall be enforced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission functions and distinct information systems support functions shall be divided among different roles, and support functions shall be performed by different individuals (e.g., personnel responsible for administering access control functions shall not also administer audit functions). Personnel developing and testing system code shall not have access to production libraries. Access control software shall be in place to limit individual authority and information access, such that the collusion of two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties.

Guidance

The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Applicability: All	References: ARS: AC-5; FISCAM: TAY-1.3.2, TSD-1.1.1, TSD-1.1.2, TSD-1.1.3, TSD-1.1.5, TSD-1.2.1, TSD-1.3.3, TSD-2.2.2, TSS-1.1.2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3; NIST 800-53/53A: AC-5; PISP: 4.1.5	Related Controls:
ASSESSMENT PROCEDURE: A	C-5.1	
Assessment Objective		
Determine if:		
0	ppropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibil	ities and duties of individuals; and
	es separation of duties through assigned access authorizations.	
Assessment Methods And Obje		
information system audit records	procedures addressing separation of duties; information system configuration settings and associated documentation; ; other relevant documents or records.	list of separation of duties authorizations;
• •	nnel with responsibilities for defining appropriate divisions of responsibility and separation of duties.(Optional)	
	plementing separation of duties policy.(Optional)	
AC-5(CMS-1) – Enhancement (M	loderate)	
Control		
Ensure that audit functions are n	ot performed by security personnel responsible for administering access control.	
Applicability: All	References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5	Related Controls:
ASSESSMENT PROCEDURE: A	C-5(CMS-1).1	
ASSESSMENT FROCEDORE. A		
Assessment Objective Determine if the organization est	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r	esponsibilities and duties of individuals.
Assessment Objective Determine if the organization est	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r	esponsibilities and duties of individuals.
Assessment Objective Determine if the organization est Assessment Methods And Obje Examine: Separation of duties p	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r ects olicy and procedures; information system configuration settings and associated documentation; list of separation of du	ties authorizations; information system audit
Assessment Objective Determine if the organization est Assessment Methods And Obje Examine: Separation of duties p records; other relevant documen	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r ects olicy and procedures; information system configuration settings and associated documentation; list of separation of du ts or records to determine if audit functions are NOT performed by security personnel responsible for administering ac	ties authorizations; information system audit
Assessment Objective Determine if the organization est Assessment Methods And Obje Examine: Separation of duties p records; other relevant documen enforces separation of duties thr	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r ects olicy and procedures; information system configuration settings and associated documentation; list of separation of du ts or records to determine if audit functions are NOT performed by security personnel responsible for administering ac bugh assigned access authorizations.	ties authorizations; information system audit cess control. Also, ensure that the organizatio
Assessment Objective Determine if the organization est Assessment Methods And Obje Examine: Separation of duties p records; other relevant documen enforces separation of duties thr Interview: Organizational person	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r ects olicy and procedures; information system configuration settings and associated documentation; list of separation of du s or records to determine if audit functions are NOT performed by security personnel responsible for administering ac bugh assigned access authorizations. anel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit	ties authorizations; information system audit cess control. Also, ensure that the organizatio
Assessment Objective Determine if the organization est Assessment Methods And Obje Examine: Separation of duties p records; other relevant documen enforces separation of duties thr Interview: Organizational person personnel. Also, determine if ac	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r ects olicy and procedures; information system configuration settings and associated documentation; list of separation of du ts or records to determine if audit functions are NOT performed by security personnel responsible for administering ac bugh assigned access authorizations.	ties authorizations; information system audit cess control. Also, ensure that the organizatio
Assessment Objective Determine if the organization est Assessment Methods And Obje Examine: Separation of duties p records; other relevant documen enforces separation of duties thr Interview: Organizational person personnel. Also, determine if ac Test: Automated mechanisms in	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r ects olicy and procedures; information system configuration settings and associated documentation; list of separation of du is or records to determine if audit functions are NOT performed by security personnel responsible for administering ac bugh assigned access authorizations. anel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit cess authorizations complement and reinforce separation of duties. applementing separation of duties policy.	ties authorizations; information system audit cess control. Also, ensure that the organization
Assessment Objective Determine if the organization est Assessment Methods And Obje Examine: Separation of duties p records; other relevant documen enforces separation of duties thr Interview: Organizational person personnel. Also, determine if ac Test: Automated mechanisms in AC-5(CMS-2) – Enhancement (N	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r ects olicy and procedures; information system configuration settings and associated documentation; list of separation of du is or records to determine if audit functions are NOT performed by security personnel responsible for administering ac bugh assigned access authorizations. anel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit cess authorizations complement and reinforce separation of duties. applementing separation of duties policy.	ties authorizations; information system audit cess control. Also, ensure that the organization
Assessment Objective Determine if the organization est Assessment Methods And Obje Examine: Separation of duties p records; other relevant documen enforces separation of duties thr Interview: Organizational person personnel. Also, determine if ac Test: Automated mechanisms in AC-5(CMS-2) – Enhancement (In Control	ablishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the r ects olicy and procedures; information system configuration settings and associated documentation; list of separation of du is or records to determine if audit functions are NOT performed by security personnel responsible for administering ac bugh assigned access authorizations. anel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit cess authorizations complement and reinforce separation of duties. applementing separation of duties policy.	ties authorizations; information system audit cess control. Also, ensure that the organization

ASSESSMENT PROCEDURE: AC-5(CMS-2).1

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. Assessment Methods And Objects

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization maintains a limited group of administrators with access based upon the users' roles and responsibilities. **Interview:** Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the number of personnel with root access is limited to only those personnel with a business need for root access.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-3) – Enhancement (Moderate)

Control

Ensure that critical mission functions and information system support functions are divided among separate individuals.

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals. Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the organization ensures that critical mission functions and information system support functions are divided among separate individuals.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-4) – Enhancement (Moderate)

Control

Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Applicability: All	References: ARS: AC-5(CMS-4); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-5(CMS-4).1		

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Test: Automated mechanisms implementing separation of duties policy.

AC-5(CMS-5) – Enhancement (Moderate)

Control

Ensure that an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.

Applicability: All	References: ARS: AC-5(CMS-5); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-5(CMS-5).1		

Assessment Objective

Determine if the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the

information system, conducts information secur	ity testing of the information system. nsibilities for defining appropriate divisions of responsibility and separation of duti	as None of these individuals or functions should be conducting
information security testing of the information sy		es. None of these individuals of functions should be conducting
Test: Automated mechanisms implementing se		
AC-5(FIS-1) – Enhancement (Moderate)		
Control		
Senior management is responsible for providing	g adequate resources and training to ensure that segregation of duty principles ar	e understood and established, enforced, and institutionalized within
the organization.		
Applicability: All	References: FISCAM: TSD-1.3.2	Related Controls:
ASSESSMENT PROCEDURE: AC-5(FIS-1).1		
Assessment Objective		
	e resources and training to ensure that segregation of duty principles are understo	ood and established, enforced, and institutionalized within the
organization.		
Assessment Methods And Objects Examine: Pertinent policies and procedures.		
· · ·	ior management has provided adequate resources and training to establish, enfo	rce, and institutionalize the principles of segregation of duties
AC-6 – Least Privilege (Moderate)		
Control		
	st restrictive set of privileges needed for the performance of authorized tasks.	
Guidance	st restrictive set of privileges needed for the performance of admonzed tasks.	
	privilege for specific duties and information systems (including specific ports, proto	ocols, and services) in accordance with risk assessments as
	zational operations, organizational assets, and individuals.	
Applicability: All	References: ARS: AC-6; FISCAM: TSD-2.1; HIPAA: 164.308(a)(3)(i), 164.308	(a)(4)(ii)(A); HSPD 7: Related Controls:
	D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2; NIST 800-53/53A: AC-6; PISP: 4.1.6	
ASSESSMENT PROCEDURE: AC-6.1		
Assessment Objective		
Determine if:		
· · · · · · · · · · · · · · · · · · ·	set of rights/privileges or accesses needed by users for the performance of specil	fied tasks; and
Assessment Methods And Objects	strictive set of rights/privileges or accesses needed by users.	
	Idressing least privilege; list of assigned access authorizations (user privileges); ir	nformation system configuration settings and associated
documentation; information system audit record		normation system configuration settings and associated
	nsibilities for defining least privileges necessary to accomplish specified tasks.(Op	ptional)
AC-6(CMS-1) – Enhancement (Moderate)		
Control		
Disable all file system access not explicitly requ	ired for system, application, and administrator functionality.	
Applicability: All	References: ARS: AC-6(CMS-1); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-6(CMS-1).	1	
Assessment Objective		
Determine if the information system enforces se	eparation of duties through assigned access authorizations.	
Assessment Methods And Objects		
	Idressing least privilege; list of assigned access authorizations (user privileges); ir is; other relevant documents or records to determine if all file system access not e	
Interview: Organizational personnel with respo determine if file system access not explicitly req	nsibilities for defining least privileges necessary to accomplish specified tasks to o quired for system, application, and administrator functionality are disabled. smit or process sensitive data to ensure that all file system access not explicitly re-	
Der 0		

disabled.		
AC-6(CMS-2) – Enhancement (Moderate)		
Control		
Contractors must be provided with minimal syste contractor's ability to adhere to and support CMS	em and physical access, and must agree to and support the CMS security requirements. The Security policy.	ne contractor selection process must assess the
Applicability: All	References: ARS: AC-6(CMS-2); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-6(CMS-2).1		
Assessment Objective		
-	paration of duties through assigned access authorizations.	
Assessment Methods And Objects		
documentation; information system audit records they've agreed to support the CMS security requ Interview: Organizational personnel with respon all file system access not explicitly required for s Test: Information system hosts that store, transm	Interssing least privilege; list of assigned access authorizations (user privileges); information a s; other relevant documents or records to determine if contractors are required to be provide irrements. The documented contractor selection process must assess the contractor's ability isibilities for defining least privileges necessary to accomplish specified tasks to determine t ystem, application, and administrator functionality is disabled. nit or process sensitive data; and that contain account information for contractors, to determ ity is disabled.	ed with minimal system and physical access, and that y to adhere to and support CMS security policy. he default access levels given to contractors. Ensure that
system, application, and administrator functional AC-6(CMS-3) – Enhancement (Moderate)	ity is disabled.	
Control		
	s to only authorized database administrators. Prevent users from accessing database data	files at the logical data view field or field-value level
Implement table-level access control.		
Applicability: All	References: ARS: AC-6(CMS-3); FISCAM: TAC-3.2.D.1, TAC-3.2.D.2, TAC-3.2.D.3, TAC	C-3.2.D.4 Related Controls:
ASSESSMENT PROCEDURE: AC-6(CMS-3).1		
Assessment Objective		
	paration of duties through assigned access authorizations.	
Assessment Methods And Objects		
documentation; information system audit records database administrators. Policies and procedure controls. Interview: Organizational personnel with respon	Bressing least privilege; list of assigned access authorizations (user privileges); information a s; other relevant documents or records to determine if the information system restricts the us s must also prevent users from accessing database data files at the logical data view, field, sibilities for defining least privileges necessary to accomplish specified tasks to determine i e administrators. Also, determine whether or not users are prevented from accessing database	se of database management utilities to only authorized or field-value levels. Implement column-level access f the information system restricts the use of database
levels. Column-level access controls must also l		
	letermine if the information system restricts the use of database management utilities to onling database data files at the logical data view, field, or field-value levels. Column-level acc	
AC-6(CMS-4) – Enhancement (Moderate)		
Control		
Ensure that only authorized users are permitted performance of job duties.	to access those files, directories, drives, workstations, servers, network shares, ports, proto	cols, and services that are expressly required for the
Applicability: All	References: ARS: AC-6(CMS-4); FISCAM: TAN-2.2.1; HIPAA: 164.312(c)(1); HSPD 7: D 1075: 5.1#1.1, 5.2#1, 5.2#2, 5.6.2.3#1	(10); IRS- Related Controls:
ASSESSMENT PROCEDURE: AC-6(CMS-4).1		
Assessment Objective		
Determine if the information system enforces sep	paration of duties through assigned access authorizations.	
Assessment Methods And Objects		
Examine: Access control policy; procedures add	Iressing least privilege; list of assigned access authorizations (user privileges); information	
	c); other relevant documents or records to determine if only authorized users are permitted to ervices that are expressly required for the performance of job duties.	o access those files, directories, drives, workstations,

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine if the default level of access for the various user types. Ensure that only access to those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties are assigned.

Test: Information system using a sample of user accounts with limited access, attempt to access files, directories, drives, workstations, servers, network shares, ports, protocols, or services that this user or user type has no access to.

AC-7 – Unsuccessful Log-on Attempts (Moderate)

Control

Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce a limit of CMS-defined consecutive invalid access attempts by a user during a specified time period. Systems shall be locked after a specified number of multiple unsuccessful log-on attempts.

Guidance

Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Applicability: All	References: ARS: AC-7; IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7	Related Controls:
ASSESSMENT PROCEDURE: AC-7.1		

Assessment Objective

Determine if:

(i) the organization defines the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur;

(ii) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period;

(iii) the organization defines the time period for lock out mode or delay period;

(iv) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; and

(v) the information system enforces the organization-selected lock out mode or delayed login prompt.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing unsuccessful logon attempts; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts.(Optional)

AC-7(0) – Enhancement (Moderate)

Control

Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user during a fifteen (15) minute time period. Require the lock out to persist for a minimum of one (1) hour.

Applicability: All	References: ARS: AC-7(0); IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7	Related Controls: AC-9
ACCECCMENT DROCEDURE: AC 7(0) 4		

ASSESSMENT PROCEDURE: AC-7(0).1

Assessment Objective

Determine if the organization configures system lockout to assist in preventing password guessing.

Assessment Methods And Objects

Examine: Password lockout policy includes failed log-on attempts, lockout timeframes period for failed attempts and system/network administrator account reset capabilities.

Interview: A sampling of users for knowledge of log-on and account lockout procedure policy is known.

Test: The account lockout function requires and administrator's reset of the locked-out user account.

AC-8 – System Use Notification (Moderate)

Control

An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS information system.

Guidance

Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is

Applicability: All	References: ARS: AC-8; FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2; NIST 800-53/53A: AC-8; PISP: 4.1.8	Related Controls: SI-4
ASSESSMENT PROCEDURE: AC-	3.1	
Assessment Objective		
Determine if:		
(i) the information system displays a	system use notification message before granting system access informing potential users:	
 that the user is accessing a U.S. G 		
- that system usage may be monitor		
	n is prohibited and subject to criminal and civil penalties;	
- that use of the system indicates co	5 5·	
	age provides appropriate privacy and security notices (based on associated privacy and security policies or summar formation system use notification message before its use; and	ies).
	age remains on the screen until the user takes explicit actions to log on to the information system.	
ssessment Methods And Objects		tion acttings and accordiated documentation
other relevant documents or records	cedures addressing system use notification; information system notification messages; information system configura	ation settings and associated documentation
	menting the access control policy for system use notification.(Optional)	
C-8(CMS-1) – Enhancement (Mod		
Control	n n a n a n a n a n a n a n a n a n a n	
	display a warning banner automatically prior to granting access to potential users. Notify users that:	
(a) They are accessing a U.S. Gove	esponsibility for its computer systems;	
	nation Security Policies, Standards, and Procedures;	
(d) Their usage may be monitored, i		
	nd subject to criminal and civil penalties; and	
	n establishes their consent to any and all monitoring and recording of their activities.	
Guidance		
All CMS information system comput	ers and network devices under their control, independently, prominently and completely display the notice and conse	ent banner immediately upon users'
authentication to the system, includi	ng, but not limited to, web, ftp, telnet, or other services accessed.	
pplicability: All	References: ARS: AC-8(CMS-1); FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.6.3.2#4.2	Related Controls:
SSESSMENT PROCEDURE: AC-	B(CMS-1).1	
ssessment Objective		
Determine if the information system	displays a system use notification message before granting system access informing potential users:	
- that the user is accessing a U.S. G	overnment information system;	
 that system usage may be monitor 		
	n is prohibited and subject to criminal and civil penalties;	
- that use of the system indicates co		
ssessment Methods And Objects		
	cedures addressing system use notification; information system notification messages; information system configura	
	to determine if the information system is configured to display a warning banner automatically prior to granting acce	ess to potential users. Notify users that:
(a) They are accessing a U.S. Gove		
(b) CMS maintains ownership and ru	notion Security Deligion, Standarda, and Bracedures;	
(c) Users must adhere to CMS Infor	nation Security Policies, Standards, and Procedures;	
(c) Users must adhere to CMS Infor (d) Their usage may be monitored, r	ecorded, and audited;	
 (c) Users must adhere to CMS Infor (d) Their usage may be monitored, i (e) Unauthorized use is prohibited a 	ecorded, and audited; nd subject to criminal and civil penalties; and	
 (c) Users must adhere to CMS Infor (d) Their usage may be monitored, r (e) Unauthorized use is prohibited a (f) The use of the information system 	ecorded, and audited; nd subject to criminal and civil penalties; and n establishes their consent to any and all monitoring and recording of their activities.	st contain the following elements:
 (c) Users must adhere to CMS Infor (d) Their usage may be monitored, i (e) Unauthorized use is prohibited a (f) The use of the information system 	ecorded, and audited; nd subject to criminal and civil penalties; and n establishes their consent to any and all monitoring and recording of their activities. to determine if hosts are configured to present a warning banner at system access points. The warning banner mu	st contain the following elements:

(b) CMS maintains ownership and responsibilit	ty for its computer systems;	
(c) Users must adhere to CMS Information Sec		
(d) Their usage may be monitored, recorded, a		
(e) Unauthorized use is prohibited and subject		
	es their consent to any and all monitoring and recording of their activities.	
- 0	ne access control policy for system use notification.	
AC-8(CMS-2) – Enhancement (Moderate)		
Control		
Develop and implement the warning banner in	conjunction with legal counsel.	
Applicability: All	References: ARS: AC-8(CMS-2); IRS-1075: 5.6.3.2#4.2	Related Controls:
ASSESSMENT PROCEDURE: AC-8(CMS-2)	.1	
Assessment Objective		
Determine if the system use notification messa	age provides appropriate privacy and security notices (based on associated privacy and se	curity policies or summaries).
Assessment Methods And Objects		,
-	ddressing system use notification; information system notification messages; information s	system configuration settings and associated documentation:
	ine if warning banners were developed and implemented in conjunction with legal counsel	
Interview: Organizational personnel to determ	ine if warning banners were developed and implemented in conjunction with legal counsel	
Test: Automated mechanisms implementing th	ne access control policy for system use notification.(Optional)	
AC-8(CMS-3) – Enhancement (Moderate)		
Control		
Post clear privacy policies on web sites, major	entry points to a web site and any web page where substantial personal information from	the public is collected.
Applicability: All	References: ARS: AC-8(CMS-3); IRS-1075: 5.6.3.2#4.2	Related Controls:
ASSESSMENT PROCEDURE: AC-8(CMS-3)		
Assessment Objective		
	age provides appropriate privacy and security notices (based on associated privacy and se	curity policies or summaries)
Assessment Methods And Objects	age provides appropriate privacy and security notices (based on associated privacy and se	curry policies of summanes).
-	ddressing system use notification; information system notification messages; information s	wetom configuration softings and associated documentation:
	ine if clear privacy policies are posted on web sites, major entry points to a web site and a	
public is collected.		ny web page where substantial personal information norm the
	ine if clear privacy policies are posted where substantial personal information from the put	blic is collected.
a 1	ne access control policy for system use notification.	
AC-10 – Concurrent Session Control (
Control		
	nit the number of concurrent user sessions, based upon the established business needs of	the upper CMS and the constitutive lovel of the CMS
information system.	in the number of concurrent user sessions, based upon the established business needs of	
Guidance		
	essions to function properly. However, based on the operational needs, automated mechar	nisme limit the number of concurrent user speciens. It is good
	hy system to have user concurrent sessions. Management should periodically review the r	
Applicability: All	References: ARS: AC-10: NIST 800-53/53A: AC-10: PISP: 4.1.10	Related Controls:
ASSESSMENT PROCEDURE: AC-10.1		Notated Controls.
Assessment Objective		
Determine if: (i) the organization defines the maximum numb	par of concurrent sessions for information system users; and	
	per of concurrent sessions for information system users; and concurrent sessions for users to the organization-defined number of sessions.	
Assessment Methods And Objects	denote in a concurrent excession control: information overteen configuration pattings and access	inted documentations information system accurity plans other
relevant documents or records.(Optional)	ddressing concurrent session control; information system configuration settings and assoc	nated documentation, information system security plan; other
Rev. 9	Page 15 of 189	BPSSM Appendix A, Attachment 2
	-	

Test: Automated mechanisms implementing th	e access control policy for concurrent session control.(Optional)	
AC-10(0) – Enhancement (Moderate)		
Control		
	on sessions is limited and enforced to one (1) session. The number of concurrent application/proces	s sessions is limited and enforced to the number of
sessions expressly required for the performanc	e of job duties.	
Applicability: All	References: ARS: AC-10(0), 4.1.10	Related Controls:
ASSESSMENT PROCEDURE: AC-10(0).1		
Assessment Objective		
	ments as specified in the baseline control and the specific CMS requirements as prescribed in this a	mplifying enhancement to the baseline control.
Assessment Methods And Objects		
	Idressing concurrent session control; information system configuration settings and associated docur	nentation; information system security plan (for
AC-10(CMS-1) – Enhancement (Moderate)	ns for information system users); other relevant documents or records.	
Control	application/process session for each upor is documented in the SSD	
Applicability: All	application/process session for each user is documented in the SSP. References: ARS: AC-10(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: AC-10(CMS-1		Related Controls.
Assessment Objective	j.1	
	umber of concurrent sessions for users to the organization-defined number of sessions.	
Assessment Methods And Objects		
-	dressing concurrent session control; information system configuration settings and associated docur	mentation: information system security plan (for
	ns for information system users); other relevant documents or records to determine if the requiremen	
log-on session for each user is documented in	•	
0 1	ne if the information system allows more than one log-on session.	
	e access control policy for concurrent session control.	
AC-11 – Session Lock (Moderate)		
Control		
Automated session lock mechanisms shall be in	n place and supporting procedures shall be developed, documented, and implemented effectively to	enable locking of the information system session
Guidance	detect inactivity and block further access until the user re-establishes the connection using proper id	entification and authentication processes.
	isms. A session lock is not a substitute for logging out of the information system. Organization-define	d time periods of inactivity comply with foderal
	emorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote a	
Applicability: All	References: ARS: AC-11; IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-11; PISP: 4.1.11	Related Controls:
ASSESSMENT PROCEDURE: AC-11.1		
Assessment Objective		
Determine if:		
() U	ser inactivity that initiates a session lock within the information system;	
· · ·	ck after the organization-defined time period of inactivity; and	
	on lock until the user reestablishes access using appropriate identification and authentication procedu	ires.
Assessment Methods And Objects	the set of second sector is the second se	and the second second state of the second state of
Examine: Access control policy; procedures ac system security plan; other relevant documents	Idressing session lock; information system design documentation; information system configuration s	settings and associated documentation; information
	e access control policy for session lock.(Optional)	
AC-11(0) – Enhancement (Moderate)		
Control		
	matically after fifteen (15) minutes of inactivity. Require a password (see IA-5, Authenticator Manage	ement) to restore local access
D 0	D 16 6100	

Applicability: All	References: ARS: AC-11(0); FISCAM: TAC-3.2.C.3; IRS-1075: 5.6.3.2#4.3, 5.7.3#1; NIST 800- 53/53A: AC-11; PISP: 4.1.11	Related Controls: IA-5
ASSESSMENT PROCEDURE: AC-11(0).1		
Assessment Objective		
	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ying enhancement to the baseline control.
Assessment Methods And Objects		
	lressing session lock; information system design documentation; information system configuration settin ne period for user inactivity after which automatic session lock is to be activated); other relevant docume	
AC-12 – Session Termination (Moderate	2)	
Control		
The information system shall identify and termina	ate all inactive remote sessions (both user and information system sessions) automatically.	
Guidance		
network (e.g., the Internet).	zational information system is accessed by a user (or an information system) communicating through a	n external, non-organization-controlled
Applicability: All	References: ARS: AC-12; FISCAM: TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-12; PISP: 4.1.12	Related Controls:
ASSESSMENT PROCEDURE: AC-12.1		
Assessment Objective		
Determine if:		
	er inactivity that initiates a remote session termination within the information system; and	
	es a remote session after the organization-defined time period of inactivity.	
Assessment Methods And Objects		
	lressing session termination; information system design documentation; information system configuratio	n settings and associated documentation;
information system security plan; other relevant		
	access control policy for session termination.(Optional)	
AC-12(0) – Enhancement (Moderate)		
Control		
	y terminate all remote sessions (user and information system) after 30 minutes of inactivity.	F
Applicability: All	References: ARS: AC-12(0); FISCAM: TAC-3.2.C.3, TAN-2.1.6; HIPAA: 164.312(a)(2)(iii); IRS-1075: 5.6.3.2#4.3; NIST 800-53/53A: AC-12; PISP: 4.1.12	Related Controls:
ASSESSMENT PROCEDURE: AC-12(0).1		
Assessment Objective		
Determine if the organization meets the requiren	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ying enhancement to the baseline control.
Assessment Methods And Objects		
	Iressing session termination; information system design documentation; information system configuration- n-defined time period for user inactivity after which automatic session termination is to be activated); oth	
AC-13 – Supervision and Review—Acce	ss Control (Moderate)	
Control		
Personnel shall be supervised and reviewed with	n respect to the usage of CMS information system access controls. Automated mechanisms shall be in n a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of us nently.	
Guidance		
The organization reviews audit records (e.g., use system-related activities and periodically reviews responsibilities. The extent of the audit record re	er activity logs) for inappropriate activities in accordance with organizational procedures. The organization changes to access authorizations. The organization reviews more frequently the activities of users with views is based on the FIPS 199 impact level of the information system. For example, for low-impact syster at central points such as a web proxy or email servers and when specific circumstances warrant rev agement.	significant information system roles and tems, it is not intended that security logs be
Rev 9	Page 17 of 189	BPSSM Appendix A Attachment 2

Applicability: All	References: ARS: AC-13; FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSD-3.2.1, TSD-3.2.3, TS 2.1.3; HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: AC-13; PISP: 4.1.13	SS- Related Controls:
ASSESSMENT PROCEDURE:		
Assessment Objective		
2	upervises and reviews the activities of users with respect to the enforcement and usage of information system acces	ss controls.
Assessment Methods And Obj		
Examine: Access control policy	; procedures addressing supervision and review of access control enforcement and usage; organizational records o	of supervisory notices of disciplinary actions to
	ption reports; other relevant documents or records.	
Interview: Organizational perso	onnel with supervisory and access control responsibilities.(Optional)	
AC-13(1) – Enhancement (Mod	erate)	
Control		
Employ automated mechanisms	s to facilitate the review of user activities.	
Applicability: All	References: ARS: AC-13(1); NIST 800-53/53A: AC-13(1)	Related Controls:
ASSESSMENT PROCEDURE: A	AC-13(1).1	
Assessment Objective		
Determine if the organization en	nploys automated mechanisms within the information system to support and facilitate the review of user activities.	
Assessment Methods And Obj	ects	
	r; procedures addressing supervision and review of access control enforcement and usage; information system des	ign documentation; information system
5 5	ciated documentation; other relevant documents or records.	
	supporting the access control policy for supervision and review of user activities.(Optional)	
C-13(CMS-1) – Enhancement	(Moderate)	
Control		
	ectories for unexpected and/or unauthorized changes at least once per day. Automate the review of file creation, ch	anges and deletions; and monitor permission
	ation for technical staff review and assessment.	
	References: ARS: AC-13(CMS-1); FISCAM: TAC-2.1.5; HIPAA: 164.312(c)(2), 164.312(e)(2)(i)	Related Controls:
ASSESSMENT PROCEDURE: A	AC-13(CMS-1).1	
Assessment Objective		
-	mploys automated mechanisms within the information system to support and facilitate the review of user activities.	
Assessment Methods And Obj		
Examine: Access control policy	r; procedures addressing supervision and review of access control enforcement and usage; organizational records or ption reports; other relevant documents or records to determine if files and directories are reviewed for unexpected and the second se	of supervisory notices of disciplinary actions to
	iges and deletions, and permission changes must be monitored automatically. Alert notifications must be generated	
	ponnel with supervisory and access control responsibilities to determine if the integrity of files and directories for une	
	on, changes and deletions, and permission changes are being reviewed automatically. Determine if alert notificatio	
being generated.		
	supporting the access control policy for supervision and review of user activities.	
AC-13(CMS-2) – Enhancement	(Moderate)	
Control		
00 0	and user account activities, failed and successful log-on, security policy modifications, use of administrator privilege	es, system shutdowns, reboots, errors and access
authorizations.		
Applicability: All	References: ARS: AC-13(CMS-2); FISCAM: TAC-2.1.5, TAN-2.1.8, TSS-2.1.3	Related Controls:
SSESSMENT PROCEDURE:	AC-13(CMS-2).1	
Assessment Objective		
5	nploys automated mechanisms within the information system to support and facilitate the review of user activities.	
Assessment Methods And Obj		
	r; procedures addressing supervision and review of access control enforcement and usage; organizational records	
	ption reports; other relevant documents or records to determine if logging of administrator and user account activitie	es, system shutdowns, reboots, errors and access
Rev. 9	Page 18 of 189	BPSSM Appendix A, Attachmen

authorizations is enabled. Interview: Organizational personnel with supervisory and access control responsibilities to determine if logging of administrator and user account activities, system shutdowns, reboots, errors and access authorizations is enabled. Test: Automated mechanisms supporting the access control policy for supervision and review of user activities. AC-13(CMS-3) – Enhancement (Moderate) Control Inspect administrator groups, root accounts and other system related accounts on demand but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created. References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3 **Related Controls:** Applicability: All ASSESSMENT PROCEDURE: AC-13(CMS-3).1 **Assessment Objective** Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities. **Assessment Methods And Objects** Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system related accounts are inspected on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created. Interview: Organizational personnel with supervisory and access control responsibilities to determine if administrator groups, root accounts and other system related accounts are inspected on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created. Test: Automated mechanisms supporting the access control policy for supervision and review of user. AC-13(FIS-1) – Enhancement (Moderate) Control Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed. References: FISCAM: TSD-1.1.4 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: AC-13(FIS-1).1 **Assessment Objective** Determine if the organizational supervisory personnel review transactions performed. **Assessment Methods And Objects** Examine: Activities and test transaction reviews. Examine: Pertinent policies and procedures. Interview: Management. AC-14 – Permitted Actions without Identification or Authentication (Moderate) Control Based upon mission / business requirements, public access to CMS information systems without identification and authorization shall be limited to public websites and other publicly available systems. CMS information systems shall be configured to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication. Guidance The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov). Applicability: All References: ARS: AC-14: NIST 800-53/53A: AC-14: PISP: 4.1.14 Related Controls: IA-2 ASSESSMENT PROCEDURE: AC-14.1 Assessment Objective Determine if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication. **Assessment Methods And Objects** Examine: Access control policy: procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records. Test: Automated mechanisms implementing the access control policy for permitted actions without identification and authentication. (Optional)

AC-14(0) – Enhancement (Moderate)		
Control		
	can be performed on the information system without identification or authentication.	
Applicability: All	References: ARS: AC-14(0); NIST 800-53/53A: AC-14; PISP: 4.1.14	Related Controls:
ASSESSMENT PROCEDURE: AC-14(0).1		
Assessment Objective		
	ents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	/ing enhancement to the baseline control.
Assessment Methods And Objects		C C
Examine: Access control policy; procedures add information system security plan; other relevant of	ressing permitted actions without identification and authentication; information system configuration sett documents or records.	ings and associated documentation;
AC-14(1) – Enhancement (Moderate)		
Control		
Ensure that public users (users who have not be information.	en authenticated) only have access to the extent necessary to accomplish mission objectives while prev	enting unauthorized access to sensitive
Applicability: All	References: ARS: AC-14(1); HIPAA: 164.312(c)(1); NIST 800-53/53A: AC-14(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-14(1).1		
Assessment Objective		
Determine if the organization permits actions to b	be performed without identification and authentication only to the extent necessary to accomplish mission	n objectives.
Assessment Methods And Objects		
	ressing permitted actions without identification and authentication; information system configuration sett	ings and associated documentation; list of
	ed without identification and authentication; other relevant documents or records.	
	sibilities for defining permitted actions without identification and authentication.(Optional)	
AC-16 – Automated Labeling (Moderate		
Control		
	"in storage," "in process," and "in transit" with special dissemination handling or distribution instructions,	in a manner consistent with this policy.
Guidance		
	internal data structures (e.g., records, files) within the information system. Information labeling is accom	plished in accordance with: (i) access control
Applicability: All	, or distribution instructions; or (iii) as otherwise required to enforce information system security policy. References: ARS: AC-16: NIST 800-53/53A: AC-16: PISP: 4.1.16	Related Controls: AC-15
ASSESSMENT PROCEDURE: AC-16.1	Reletences. ARS. AC-10, NIS1 600-55/55A. AC-10, FISF. 4.1.10	Related Controls. AC-15
Assessment Objective	I labels information in starson in process, and in transmission	
Assessment Methods And Objects	/ labels information in storage, in process, and in transmission.	
	ressing automated (internal) labeling of information within the information system; information system de	sign documentation: information system
	tion; other relevant documents or records.(Optional)	sign documentation, information system
	omated (internal) labeling within the information system.(Optional)	
AC-16(CMS-1) – Enhancement (Moderate)		
Control		
	re that information in storage, in process, and in transmission is labeled appropriately and in accordance	e with CMS policy (e.g., sensitive information
is labeled as such and instructs / requires specia		
Applicability: All	References: ARS: AC-16(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: AC-16(CMS-1).	1	
Assessment Objective		
Determine if the information system appropriately	labels information in storage, in process, and in transmission.	
Assessment Methods And Objects		
Examine: Access control policy; procedures add	ressing automated (internal) labeling of information within the information system; information system de	sign documentation; information system

configuration settings and associated documentation; other relevant documents or records to determine, if automated information labeling is utilized, ensure that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

Interview: Organization personnel to determine, if automated information labeling is utilized, that information in storage, in process, and in transmission is labeled appropriately and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires special handling).

Test: Automated mechanisms implementing automated (internal) labeling within the information system.

AC-17 – Remote Access (Moderate)

Control

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can access the information system from remote locations shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Dial-up lines, other than those with FIPS 140 (as amended) validated cryptography, shall not be used to gain access to a CMS information system that processes CMS sensitive information unless the CIO or his/her designated representative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dialup capabilities.

Guidance

Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST SP 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73 and 800-78. NIST SP 800-77 provides guidance on IPSec-based virtual private networks.

 Applicability: All
 References: ARS: AC-17; FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC-17; PISP: 4.1.17
 Related Controls: IA-2, SC-9

ASSESSMENT PROCEDURE: AC-17.1

Assessment Objective

Determine if the organization documents, monitors, and controls all methods of remote access to the information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities.

AC-17(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to facilitate the monitoring and control of remote access methods.

Applicability: All	References: ARS: AC-17(1); IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-17(1).1		

Assessment Objective

Determine if the information system employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing the access control policy for remote access.(Optional)

AC-17(2) – Enhancement (Moderate)		_
Control		
Employ cryptography to protect the confidentialit	ty and integrity of remote access sessions.	
Applicability: All	References: ARS: AC-17(2); FISCAM: TAC-3.3; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-53/53A: AC- Related C	Controls:
	17(2)	

ASSESSMENT PROCEDURE: AC-17(2).1		
Assessment Objective		
Determine if the information system employs cry	ptography to protect the confidentiality and integrity of remote access sessions.	
Assessment Methods And Objects		
Examine: Access control policy; procedures add	ressing remote access to the information system; information system design documentation; information	n system configuration settings and associated
documentation; other relevant documents or reco		, , , , , , , , , , , , , , , , , , , ,
Test: Automated mechanisms implementing cryp	otographic protections for remote access.(Optional)	
AC-17(3) – Enhancement (Moderate)		
Control		
Control all remote access through a limited numb	per of managed access control points.	
Applicability: All	References: ARS: AC-17(3); IRS-1075: 5.6.3.2#5; NIST 800-53/53A: AC-17(3)	Related Controls:
ASSESSMENT PROCEDURE: AC-17(3).1		
Assessment Objective		
Determine if:		
(i) the organization defines managed access con	trol points for remote access to the information system; and	
(ii) the information system controls all remote acc	cesses through a limited number of managed access control points.	
Assessment Methods And Objects		
-	ressing remote access to the information system; information system design documentation; list of man	aged access control points; information
system configuration settings and associated do	cumentation; information system audit records; other relevant documents or records.	-
Test: Automated mechanisms implementing the	access control policy for remote access.(Optional)	
AC-17(4) – Enhancement (Moderate)		
Control		
Permit remote access for privileged functions on	ly for compelling operational needs and document the rationale for such access in the security plan for t	he information system.
Applicability: All	References: ARS: AC-17(4); FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5; NIST 800-53/53A:	Related Controls:
	AC-17(4)	
ASSESSMENT PROCEDURE: AC-17(4).1		
Assessment Objective		
Determine if:		
	mpelling operational needs when remote access to privileged functions on the information system is allo	
· · · · · · · · · · · · · · · · · · ·	ivileged functions only for compelling operational needs and documents the rationale for such access in	the security plan for the information system.
Assessment Methods And Objects		
	Iressing remote access to the information system; information system configuration settings and associa	ated documentation; information system
security plan; information system audit records; o		
	access control policy for remote access.(Optional)	
AC-17(CMS-1) – Enhancement (Moderate)		
Control		
	VPN link(s) if connected to the information system and using remote administration. Utilize an approve password authentication or additional authentication protection (e.g., token-based).	d encryption standard (see SC-13, Use of
Applicability: All	References: ARS: AC-17(CMS-1); IRS-1075: 5.6.3.2#5	Related Controls: SC-13
ASSESSMENT PROCEDURE: AC-17(CMS-1).	1	
Assessment Objective		
	rs, and controls all methods of remote access to the information system.	
Assessment Methods And Objects		
Examine: Access control policy; procedures add documentation; information system audit records	Iressing remote access to the information system; list of information system accounts; information system s; other relevant documents or records to determine if secure management protocols through a VPN link n that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination equired to access system.	(s) if connected to the information system and
Rev Q	Page 22 of 180	BPSSM Appendix A Attachment

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if secure management protocols through a VPN link(s) if connected to the information system and using remote administration are enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system. Test: Automated mechanisms implementing the access control policy for remote access to determine that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4.16.13) in combination with password authentication or additional authentication protection (e.g., token-based) is required to access system. AC-17(CMS-2) – Enhancement (Moderate) Control Implement password protection for remote access connections. Applicability: All References: ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5 **Related Controls:** ASSESSMENT PROCEDURE: AC-17(CMS-2).1 Assessment Objective Determine if the organization documents, monitors, and controls all methods of remote access to the information system. Assessment Methods And Objects Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if password protection for remote access connections is implemented. Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if password protection is required for remote access connections. Test: Automated mechanisms implementing the access control policy for remote access to determine remote access connections by attempting to gain access without a password. AC-17(CMS-3) – Enhancement (Moderate) Control Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) cannot be used. References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075; 5.6.3.2#5 Applicability: All Related Controls: ASSESSMENT PROCEDURE: AC-17(CMS-3).1 **Assessment Objective** Determine if: (i) the organization defines managed access control points for remote access to the information system; and (ii) the information system controls all remote accesses through a limited number of managed access control points. Assessment Methods And Objects Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified annually. Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually. Test: Automated mechanisms implementing the access control policy for remote access to determine if the information system requires callback capability with re-authentication to verify connections from authorized locations when MDCN cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor should be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems should be authorized and logged. User IDs assigned to vendors will be recertified annually. AC-17(CMS-4) – Enhancement (Moderate) Control If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix A for e-Authentication standards. Applicability: All References: ARS: AC-17(CMS-4); IRS-1075: 5.6.3.2#5 **Related Controls:** ASSESSMENT PROCEDURE: AC-17(CMS-4).1 Assessment Objective Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions. Assessment Methods And Objects Examine: Access control policy; procedures addressing remote access to the information system; list of information system accounts; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if e-authentication is implemented as a remote access solution or associated with remote access. If so, refer to ARS Appendix A for e-Authentication standards. Rev. 9 Page 23 of 189 **BPSSM** Appendix A, Attachment 2

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities to determine if the informati Appendix A for e-Authentication standards.	ion system implements e-authentication. If so, refer to AR
Test: Automated mechanisms implementing the access control policy for remote access to determine if e-authentication is implemented. standards.	If so, refer to ARS Appendix A for e-Authentication
C-17(FIS-1) – Enhancement (Moderate)	
Control	
Remote access phone numbers are not published and are periodically changed.	
pplicability: All References: FISCAM: TAC-3.2.E.2.2	Related Controls:
SSESSMENT PROCEDURE: AC-17(FIS-1).1	
ssessment Objective	
Determine if the organization changes, periodically, remote access phone numbers and those phone numbers are not published.	
ssessment Methods And Objects	
Examine: Documentation showing changes to dial-in numbers.	
Examine: Entity's telephone directory to verify that the numbers are not listed.	
Examine: Pertinent policies and procedures.	
Interview: Remote access users.	
C-18 – Wireless Access Restrictions (Moderate)	
ontrol	
Installation of wireless access points (WAP) into CMS information systems and networks shall be prohibited unless explicitly authorized, ir	
representative. Authorized WAP devices and wireless access shall be monitored on a regular basis, and wireless communications shall be	be secured through the use of approved encryption control
uidance	
NIST SP 800-48 and 800-97 provide guidance on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion dete	
pplicability: All References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18	Related Controls:
SSESSMENT PROCEDURE: AC-18.1	
ssessment Objective	
Determine if:	
(i) the organization establishes usage restrictions and implementation guidance for wireless technologies;	
(ii) the organization authorizes, monitors, and controls wireless access to the information system; and	
(iii) the wireless access restrictions are consistent with NIST SP 800-48 and 800-97.	
ssessment Methods And Objects Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and	900 07. activities related to wireless outbarization
monitoring, and control; information system audit records; other relevant documents or records.	
Test: Wireless access usage and restrictions.	
C-18(0) – Enhancement (Moderate)	
ontrol	
CMS policy prohibits the use of wireless access unless explicitly approved by the CMS CIO or his/her designated representative.	
pplicability: All References: ARS: AC-18(0); NIST 800-53/53A: AC-18; PISP: 4.1.18	Related Controls:
SSESSMENT PROCEDURE: AC-18(0).1	Related Controls.
ssessment Objective	
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribe	d in this amplifying enhancement to the baseline control
seessment Methods And Objects	
Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and	800-97: activities related to wireless authorization
	out-or, activities related to wireless authorization,
monitoring, and control; information system audit records; other relevant documents or records.	

AC-18(1) – Enhancement (Moderate)	
Control	
If wireless access is explicitly approved, approved authentication and encryption is used to protect wireless access to the information	n system.
Applicability: All References: ARS: AC-18(1); NIST 800-53/53A: AC-18(1)	Related Controls:
ASSESSMENT PROCEDURE: AC-18(1).1	
Assessment Objective	
Determine if the organization uses authentication and encryption to protect wireless access to the information system.	
Assessment Methods And Objects	
Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); information syst settings and associated documentation; information system audit records; other relevant documents or records.	tem design documentation; information system configuration
Test: Automated mechanisms implementing the access control policy for wireless access to the information system. (Optional)	
AC-18(2) – Enhancement (Moderate)	
Control	
Perform quarterly scans for unauthorized wireless access points and take appropriate action if any access points are discovered.	
Guidance	
Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information system containing the high-impact information systems.	ms. The scan is not limited to only those areas within the facility
Applicability: All References: ARS: AC-18(2)	Related Controls:
ASSESSMENT PROCEDURE: AC-18(2).1	
Assessment Objective	
Determine if:	
(i) the organization defines the frequency of scans for unauthorized wireless access points; and	
(ii) the organization scans for unauthorized wireless access points in accordance with organization-defined frequency and takes app	propriate action if such an access points are discovered.
Assessment Methods And Objects	
Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning	ng reports: other relevant documents or records.(Optional)
Test: Scanning procedure for unauthorized wireless access points.(Optional)	······································
AC-18(DIR-1) – Enhancement (Moderate)	
Control	
If wireless access is explicitly approved, wireless devices, service set identifier broadcasting is disabled and the following wireless a	cosse controls are implemented:
(a) encryption protection is enabled;	ccess controis are implemented.
(b) access points are placed in secure areas;	
(c) access points are shut down when not in use (i.e., nights, weekends);	
(d) a firewall is implemented between the wireless network and the wired infrastructure;	
(e) MAC address authentication is utilized;	
(f) static IP addresses, not DHCP, is utilized;	
(g) personal firewalls are utilized on all wireless clients;	
(ĥ) file sharing is disabled on all wireless clients;	
(i) Intrusion detection agents are deployed on the wireless side of the firewall; and	
(j) wireless activity is monitored and recorded, and the records are reviewed on a regular basis.	
Applicability: All References:	Related Controls:
ASSESSMENT PROCEDURE: AC-18(DIR-1).1	
Assessment Objective	
Determine if the organization establishes wireless policies and strict procedures that control access to the wireless LAN and separat	tes/restricts the wireless LAN from the wired network infrastruct
Assessment Methods And Objects	
Examine: Access control procedures for continuous wireless intrusion monitoring of approved and operational wireless systems.	
Interview: Staff personnel who review the wireless LAN records know what to look for in the data for an unauthorized intrusion, and intrusion is detected.	the staff knows the reporting procedures when an unauthorized

Test: The wireless LAN does not allow roque wireless devices into the approved wireless network infrastructure. AC-19 – Access Control for Portable and Mobile Devices (Moderate) Control The connection of portable and mobile devices (e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CIO or his/her designated representative. Prior to connecting portable and mobile devices to CMS information systems and networks, such devices shall be configured to comply with CMS IS policies and procedures. The storage and transmission of CMS sensitive information on portable and mobile information devices shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware. The activities and controls shall be commensurate with the system security level of the information. Guidance Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Applicability: All References: ARS: AC-19: IRS-1075: 4.6#1: NIST 800-53/53A: AC-19: PISP: 4.1.19 Related Controls: MP-4, MP-5 **ASSESSMENT PROCEDURE: AC-19.1 Assessment Objective** Determine if: (i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices; (ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (iii) the organization authorizes, monitors, and controls device access to organizational information systems, **Assessment Methods And Objects** Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation: information system audit records; other relevant documents or records. Interview: Organizational personnel who use portable and mobile devices to access the information system. Test: Automated mechanisms implementing access control policy for portable and mobile devices.(Optional) AC-19(CMS-1) – Enhancement (Moderate) Control If portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative: Employ an approved method of cryptography (see SC-13. Use of Cryptography, PISP 4.16.13) to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops. Applicability: All References: ARS: AC-19(CMS-1); FISCAM: TAC-3.3; IRS-1075: 4.6#1, 4.7.2#1 Related Controls: MA-CMS-1, MA-CMS-2, SC-13 ASSESSMENT PROCEDURE: AC-19(CMS-1).1 **Assessment Objective** Determine if: (i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices; (ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (iii) the organization authorizes, monitors, and controls device access to organizational information systems. Assessment Methods And Objects Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization,

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records to determine if portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in writing by the CIO or his/her designated representative. Also, determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Interview: Organizational personnel who use portable and mobile devices to access the information system to determine if portable and/or mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are authorized in

writing by the CIO or his/her designated representative. Also, determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

Test: Automated mechanisms implementing access control policy for portable and mobile devices to determine if an approved method of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) is employed to protect information residing on portable and mobile information devices and utilize whole-disk encryption solution for laptops.

AC-20 – Use of External Information Systems (Moderate)

Control

External information systems, including, but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports shall not be used to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative.

Strict terms and conditions shall be established for the use of external information systems. The terms and conditions shall address, at a minimum:

4.1.20.1. The types of applications that can be accessed from external information systems;

4.1.20.2. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;

4.1.20.3. How other users of the external information system will be prevented from accessing federal information;

4.1.20.4. The use of virtual private networking (VPN) and firewall technologies;

4.1.20.5. The use of and protection against the vulnerabilities of wireless technologies;

4.1.20.6. The maintenance of adequate physical security controls;

4.1.20.7. The use of virus and spyware protection software; and

4.1.20.8. How often the security capabilities of installed software are to be updated.

Guidance

External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Applicability: All	References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: A0 4.1.20	C-20; PISP:	Related Controls:

ASSESSMENT PROCEDURE: AC-20.1

Assessment Objective

Determine if:

(i) the organization defines the types of applications that can be accessed from the external information system;

(ii) the organization defines the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system; and

(iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel who use external information systems to access the information system.(Optional)

AC-20(1) – Enhancement (Moderate)

Control

Users are prohibited from using any external information system to access the information system or to process, store, or transmit CMS-controlled information except in situations where the organization:

(a) Can verify the employment of required security controls on the external system as specified in CMS' information security policy and the organization's system security plan; or

Applicability: All	tem connection or processing agreements with the organizational entity hosting the external information References: ARS: AC-20(1); IRS-1075: 4.7.2#1; NIST 800-53/53A: AC-20(1)	Related Controls:
ASSESSMENT PROCEDURE: A	C-20(1).1	
Assessment Objective		
-	hibits authorized individuals from using an external information system to access the information syst	em or to process, store, or transmit organization-controlled
information except in situations v		······································
	ns, the employment of required security controls on the external system as specified in the organizati	on's information security policy and system security plan whe
allowing connections to the external		
 approves, for authorized exception 	tions, information system connection or processing agreements with the organizational entity hosting	the external information system.
Assessment Methods And Obje	cts	
Examine: Access control policy;	procedures addressing the use of external information systems; information system security plan; inf	ormation system configuration settings and associated
documentation; information syste	m connection or processing agreements; account management documents; other relevant document	ts or records.
AC-20(CMS-1) – Enhancement	Moderate)	
Control		
	m home to implement fundamental security controls and practices, including passwords, virus protect	tion, and personal firewalls. Limit remote access only to
	y home users to complete job duties. Require that any government-owned equipment be used only f	
Applicability: All	References: ARS: AC-20(CMS-1); IRS-1075: 4.7.2#1, 4.7.3#3	Related Controls:
ASSESSMENT PROCEDURE: A	C-20(CMS-1).1	
Assessment Objective		
-	ablishes terms and conditions for authorized individuals to access the information system from an ext	ternal information system that include the types of applications
	anizational information system from the external information system and the maximum FIPS 199 sect	
transmitted on the external inform		,,
Assessment Methods And Obje	cts	
	procedures addressing the use of external information systems; external information systems terms	and conditions: list of types of applications accessible from
external information systems; ma	ximum FIPS 199 impact level for information processed, stored, or transmitted on external informatic	on systems; information system configuration settings and
associated documentation; other	relevant documents or records to determine if the organization instructs all personnel working from h	ome to implement fundamental security controls and practice
	ction, and personal firewalls. Remote access must be limited only to information resources required b	y home users to complete job duties. Any government-owned
	business purposes by authorized employees.	
	nnel who use external information systems to access the information system to determine if the organ	
	d practices, including passwords, virus protection, and personal firewalls. Remote access must be lin	nited only to information resources required by home users to
	nent-owned equipment must be used only for business purposes by authorized employees.	
AC-20(PII-1) – Enhancement (M	bderate)	
Control		
Only organization owned compu	ers and software can be used to process, access, and store PII.	
Applicability: All	References: IRS-1075: 4.7.1#1	Related Controls:
ASSESSMENT PROCEDURE: A	C-20(PII-1).1	
Assessment Objective		
	omputers and software are owned by that organization that processes, accesses and stores PII.	
Assessment Methods And Obje		
	ter and software purchase orders indicating ownership of computers and software used to process, a	cress and store PII
	dicating that only organizational owned computers and software are used to process, access and sto	
AC-CMS-1 – System Boot A		
Control	mitted only for compelling operational needs, shall be strictly controlled, and must be approved in writ	
System boot access shall be per		
System boot access shall be per number of users who can alter o	perform non-standard boots of systems and/or components of the information system shall be limite	
System boot access shall be per		
System boot access shall be per number of users who can alter o		
System boot access shall be per number of users who can alter o		

Guidance	
When a person has unrestrained physical access to any computing system or network device the person has control of the equipment.	
If the person does not have the capability to locally access the information system's data though the boot process this can assist in protect	ting the data from loss or unauthorized access to the data
Note: Even though the system root access may be protected by privilege access controls a miss configured system can allow the system	
unauthorized media. An example of this is a LINUX system, not configured correctly, when CONT+ALT+DEL is issued from the keyboard	the equipment will re-boot automatically.
pplicability: All References: ARS: AC-CMS-1; PISP: 4.1.21	Related Controls:
SSESSMENT PROCEDURE: AC-CMS-1.1	
ssessment Objective	
Determine if the organization assesses the need for system boot access and if necessary controls, documents and monitors the continued	I need for system boot access.
ssessment Methods And Objects	
Examine: System boot access documentation to determine that there is or is not a need for boot access.	
Interview: Organizational personnel to determine that there is or is not a need for system boot access.	
C-CMS-1(CMS-1) – Enhancement (Moderate)	
Control	
If not explicitly required, boot access to removable media drives is disabled.	
Applicability: All References: ARS: AC-CMS-1(CMS-1)	Related Controls:
SSESSMENT PROCEDURE: AC-CMS-1(CMS-1).1	
Assessment Objective	
Determine if the organization evaluates the need for system boot access by removable media drives.	
ssessment Methods And Objects	
Examine: System boot access documentation to determine that, if not explicitly required, boot access to removable media drives is disable	ed.
Interview: Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled.	
Test: Information system sample of workstations to determine if boot access to removable media drives is disabled.	
\C-CMS-1(CMS-2) – Enhancement (Moderate)	
Control	
System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).	
Applicability: All References: ARS: AC-CMS-1(CMS-2)	Related Controls: IA-5
SSESSMENT PROCEDURE: AC-CMS-1(CMS-2).1	
Assessment Objective	
Determine if the organization controls access to the system BIOS when unauthorized personnel may be in physical proximity to the system	n.
Assessment Methods And Objects	
Examine: System BIOS documentation to determine if System BIOS settings are locked and BIOS access is protected by password (see	IA-5, Authenticator Management).
Interview: Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled.	
Test: Information system sample of workstations by attempting to access the System BIOS. Ensure that access to the System BIOS is pr	otected by password.
C-CMS-1(CMS-3) – Enhancement (Moderate)	
Control	
If not explicitly required, removable media drive functionality is disabled.	
pplicability: All References: ARS: AC-CMS-1(CMS-3)	Related Controls:
SSESSMENT PROCEDURE: AC-CMS-1(CMS-3).1	
ssessment Objective	
Assessment Objective Determine if the organization disables removable media drive functionality If not explicitly required.	
ssessment Objective Determine if the organization disables removable media drive functionality If not explicitly required. ssessment Methods And Objects	ed.
Assessment Objective	ed.

Awareness and Training (AT) – Operational

AT-1 – Security Awareness and Training Policy and Procedures (Moderate)

Control

An IS AT program shall be developed, documented, and implemented effectively for all personnel, including contractors and any other users of CMS information and information systems. The IS AT program shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information, information systems, and networks.

Guidance

The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-16 and 800-50 provide guidance on security awareness and training. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: AT-1; FISCAM: TSP-4.2.2; IRS-1075: 5.6.2.7#1.1-2, 6.1#1; NIST 800-53/53A: AT-1; PISP: 4.2.1	Related Controls:
A COFOONENT DROOFDURE AT 4.4		

ASSESSMENT PROCEDURE: AT-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security awareness and training policy and procedures;

(ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review security awareness and training policy and procedures; and

(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.

Interview: Organizational personnel with security awareness and training responsibilities.(Optional)

ASSESSMENT PROCEDURE: AT-1.2

Assessment Objective

Determine if:

(i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with security awareness and training responsibilities.(Optional)

AT-2 – Security Awareness (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS AT program shall be consistent with 5 CFR Part 930 (http://opm.gov/fedregis/2004/69-061404-32835-a.pdf) and the guidance provided in NIST SP 800-50.

Guidance

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	References: ARS: AT-2; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3; NIST 800-53/53A: AT-2; PISP: 4.2.2	Related Controls:
ASSESSMENT PROCEDURE: AT-2.1		

ASSESSMENT PROCEDORE. AT

Assessment Objective

(i) the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required			
by system changes; (ii) the security awareness training is consistent with applicable regulations and NIST SP 800-50;			
	s address the specific requirements of the organization and the information systems to which personnel l	nave authorized access:	
(iv) the organization defines the frequency of ref		,	
(v) the organization provides refresher security a	wareness training in accordance with organization-defined frequency, at least annually.		
Assessment Methods And Objects			
training curriculum; security awareness training	y; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate cod materials; information system security plan; other relevant documents or records.	es of federal regulations; security awareness	
	the general information system user community.(Optional)		
AT-2(0) – Enhancement (Moderate)			
Control			
changes; and every 365 days thereafter.	s and senior executives) receive basic information security awareness training prior to accessing any sys		
Applicability: All	References: ARS: AT-2(0); FISCAM: TSP-3.3.1; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3, 6.2#1.1-2, 6.2#1.4, 6.2#2.1; NIST 800-53/53A: AT-2; PISP: 4.2.2	Related Controls:	
ASSESSMENT PROCEDURE: AT-2(0).1			
Assessment Objective			
. .	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ving enhancement to the baseline control.	
Assessment Methods And Objects			
	y; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate cod		
records.	materials; information system security plan (for organization-defined frequency of refresher security awar	eness training); other relevant documents or	
AT-2(CMS-1) – Enhancement (Moderate)			
Control			
Establish a program to promote continuing awar	eness of information security issues and threats		
Applicability: All	References: ARS: AT-2(CMS-1); HIPAA: 164.308(a)(5)(ii)(A); IRS-1075: 5.6.2.7#1.3	Related Controls:	
ASSESSMENT PROCEDURE: AT-2(CMS-1).1			
Assessment Objective			
Determine if the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes.			
Assessment Methods And Objects			
	y and procedures; other relevant documents or records to determine that a program to promote continuir	ng awareness of information security issues	
Examine: Security awareness and training polic and threats has been established.	y and procedures; other relevant documents or records to determine that a program to promote continuir y awareness and training responsibilities to determine that a program to promote continuing awareness	-	
Examine: Security awareness and training polic and threats has been established. Interview: Organizational personnel with securit			
Examine: Security awareness and training polic and threats has been established. Interview: Organizational personnel with securit been established.		-	
 Examine: Security awareness and training polic and threats has been established. Interview: Organizational personnel with securit been established. AT-3 – Security Training (Moderate) Control The organization shall identify and document all significant information system security responsite 	y awareness and training responsibilities to determine that a program to promote continuing awareness positions and/or roles with significant information system security responsibilities during the system deve ilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50.	of information security issues and threats has elopment life cycle. All personnel with Content of the security awareness training	
 Examine: Security awareness and training polic and threats has been established. Interview: Organizational personnel with securit been established. AT-3 – Security Training (Moderate) Control The organization shall identify and document all significant information system security responsite 	y awareness and training responsibilities to determine that a program to promote continuing awareness of positions and/or roles with significant information system security responsibilities during the system deversibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Consystems to which personnel have authorized access. The employee shall acknowledge having received	of information security issues and threats has elopment life cycle. All personnel with Content of the security awareness training	
 Examine: Security awareness and training polic and threats has been established. Interview: Organizational personnel with securit been established. AT-3 – Security Training (Moderate) Control The organization shall identify and document all significant information system security responsit shall be determined based upon the information 	y awareness and training responsibilities to determine that a program to promote continuing awareness of positions and/or roles with significant information system security responsibilities during the system deversibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Consystems to which personnel have authorized access. The employee shall acknowledge having received	of information security issues and threats has elopment life cycle. All personnel with Content of the security awareness training	
 Examine: Security awareness and training polic and threats has been established. Interview: Organizational personnel with securit been established. AT-3 – Security Training (Moderate) Control The organization shall identify and document all significant information system security responsit shall be determined based upon the information writing or electronically as part of the training con Guidance The organization determines the appropriate con 	y awareness and training responsibilities to determine that a program to promote continuing awareness of positions and/or roles with significant information system security responsibilities during the system deversibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Consistents to which personnel have authorized access. The employee shall acknowledge having received are completion.	of information security issues and threats has elopment life cycle. All personnel with content of the security awareness training the security and awareness training either in ms to which personnel have authorized	
 Examine: Security awareness and training polic and threats has been established. Interview: Organizational personnel with securit been established. AT-3 – Security Training (Moderate) Control The organization shall identify and document all significant information system security responsit shall be determined based upon the information writing or electronically as part of the training col Guidance The organization determines the appropriate cor access. In addition, the organization provides sy perform their assigned duties. The organization's 	y awareness and training responsibilities to determine that a program to promote continuing awareness of positions and/or roles with significant information system security responsibilities during the system deversibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. C systems to which personnel have authorized access. The employee shall acknowledge having received arse completion.	of information security issues and threats has elopment life cycle. All personnel with content of the security awareness training the security and awareness training either in ms to which personnel have authorized software, adequate technical training to	
Examine: Security awareness and training polic and threats has been established. Interview: Organizational personnel with securit been established. AT-3 – Security Training (Moderate) Control The organization shall identify and document all significant information system security responsit shall be determined based upon the information writing or electronically as part of the training col Guidance The organization determines the appropriate cor access. In addition, the organization provides sy	y awareness and training responsibilities to determine that a program to promote continuing awareness of positions and/or roles with significant information system security responsibilities during the system deversibilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. Consistents to which personnel have authorized access. The employee shall acknowledge having received urse completion.	of information security issues and threats has elopment life cycle. All personnel with Content of the security awareness training the security and awareness training either in ms to which personnel have authorized software, adequate technical training to	

ASSESSMENT PROCEDURE: AT-3.1

Assessment Objective

Determine if:

(i) the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities;

(ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes;

(iii) the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security;

(iv) the security training is consistent with applicable regulations and NIST SP 800-50;

(v) the organization defines the frequency of refresher security training; and

(vi) the organization provides refresher security training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan; other relevant documents or records.

Interview: Organizational personnel with significant information system security responsibilities.(Optional)

AT-3(0) – Enhancement (Moderate)

Control

Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to CMS networks, systems, and/or applications; when required by system changes; and refresher training every 365 days thereafter.

Applicability: All	References: ARS: AT-3(0); FISCAM: TSP-3.3.1; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	Related Controls:
ACCECCMENT DROCEDURE, AT 2/0) 4		

ASSESSMENT PROCEDURE: AT-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan (for organization-defined frequency of refresher security training); other relevant documents or records.

AT-4 – Security Training Records (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that individual IS training activities, including basic security awareness training and specific information system security training, are properly documented and monitored.

Guidance

Procedures and training implementation should:

(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:

(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.

(2) Executives must receive training in information security basics and policy level training in security planning and management.

(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.

(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.

(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.

(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.

(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process. (d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	References: ARS: AT-4; FISCAM: TSP-4.2.3; IRS-1075: 6.2#1.3; NIST 800-53/53A: AT-4; PISP: 4.2.4	Related Controls:	
ASSESSMENT PROCEDURE: AT-4.1			
Assessment Objective			
	ments basic security awareness training and specific information system security training.		
Assessment Methods And Objects			
· · · · · · · · · · · · · · · · · · ·	y; procedures addressing security training records; security awareness and training records; other relevant	ant documents or records.	
AT-5 – Contacts with Security Groups a	nd Associations (Moderate)		
Control			
Contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations shall be encouraged and supported to enable security personnel to stay up to date with the latest recommended security practices, techniques, and technologies; and to share the latest security-related information including threats, vulnerabilities, and incidents.			
Guidance			
To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.			
Applicability: All	References: ARS: AT-5; HSPD 7: H(25); NIST 800-53/53A: AT-5; PISP: 4.2.5	Related Controls:	
ASSESSMENT PROCEDURE: AT-5.1			
Assessment Objective			
Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security techniques and technologies and to share security-related information.			
Assessment Methods And Objects	Assessment Methods And Objects		

Examine: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records.(Optional)

Audit and Accountability (AU) – Technical

AU-1 – Audit and Accountability Policy and Procedures (Moderate)				
Control				
	All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the			
	Is, and shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, stand	lards, and guidance; and shall be reviewed		
periodically, and, if necessary, updated.				
Guidance				
	es are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, an			
	rmation security policy for the organization. Audit and accountability procedures can be developed for the	e security program in general, and for a		
Applicability: All	ST SP 800-12 provides guidance on security policies and procedures. References: ARS: AU-1; IRS-1075: 5.6.3.3#1; NIST 800-53/53A: AU-1; PISP: 4.3.1	Related Controls:		
ASSESSMENT PROCEDURE: AU-1.1	Reletences. ARS. AU-1, IRS-10/5. 5.0.5.3#1, NIST 600-55/55A. AU-1, PISP. 4.5.1	Related Controls.		
Assessment Objective				
Determine if:	it and accountability policy and preseduracy			
(i) the organization develops and documents aud	untability policy and procedures to appropriate elements within the organization;			
	riodically review audit and accountability policy and procedures; and			
	policy and procedures when organizational review indicates updates are required.			
Assessment Methods And Objects				
Examine: Audit and accountability policy and pro	ocedures: other relevant documents or records			
Interview: Organizational personnel with audit a				
ASSESSMENT PROCEDURE: AU-1.2				
Assessment Objective				
Determine if:				
	(i) the audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;			
(ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and				
(iii) the audit and accountability procedures addre	ess all areas identified in the audit and accountability policy and address achieving policy-compliant imp	ementations of all associated security		
controls.				
Assessment Methods And Objects				
	Examine: Audit and accountability policy and procedures; other relevant documents or records.			
Interview: Organizational personnel with audit and accountability responsibilities.(Optional)				
AU-2 – Auditable Events (Moderate)				
Control				
Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security				
	incidents. The selection of auditable events shall be based upon a risk assessment as to which events require auditing on a continuous basis, and which events require auditing in response to			
specific situations.				
Guidance				
	t events which need to be audited as significant and relevant to the security of the information system.			
	Auditing activity can affect information system performance. Therefore, the organization decides, based require auditing in response to specific situations. Audit records can be generated at various levels of a			
	ght level of abstraction for audit record generation is a critical aspect of an audit capability and can facili			
problems. Additionally, the security audit function	problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of			
information to be recorded by each function. The	information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines			
auditable events that are adequate to support after-the-fact investigations of security incidents. NIST SP 800-92 provides guidance on computer security log management.				
Applicability: All	References: ARS: AU-2; FISCAM: TAC-4.3.4, TSD-3.2.2; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b);	Related Controls: AU-4		
	IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2; PISP: 4.3.2			

ASSESSMENT PROCEDURE: AU-2.1		
Assessment Objective		
Determine if:		
(i) the organization defines information system	auditable events;	
(ii) the organization-defined auditable events a	re adequate to support after-the-fact investigations of security incidents; and	
	ords for the organization-defined auditable events.	
Assessment Methods And Objects	-	
Examine: Audit and accountability policy; proc	edures addressing auditable events; information system security plan; information system configuration s	ettings and associated documentation;
information system audit records; other relevar		0
Test: Automated mechanisms implementing in	formation system auditing of organization-defined auditable events.(Optional)	
AU-2(0) – Enhancement (Moderate)		
Control		
Generate audit records for the following events	s:	
(a) User account management activities,		
(b) System shutdown,		
(c) System reboot,		
(d) System errors,		
(e) Application shutdown,		
(f) Application restart,		
(g) Application errors, (h) File creation,		
(i) File deletion,		
(j) File modification,		
(k) Failed and successful log-ons,		
(I) Security policy modifications, and		
(m) Use of administrator privileges.		
Guidance		
Note: For FTI, generate audit records for the fo	Ilowing events in addition to those specified in other controls:	
(a) All successful and unsuccessful authorization		
(b) All changes to logical access control author		
	npromise the integrity of audit policy configurations, security policy configurations and audit record genera	ation services.
(d) The audit trail shall capture the enabling or		
	changes, batch file changes and queries made to the system (e.g., operating system, application, and dat	
Applicability: All	References: ARS: AU-2(0); FISCAM: TAC-2.1.5, TAC-4.1, TSD-3.2.4; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3; NIST 800-53/53A: AU-2; PISP: 4.3.2	Related Controls:
ASSESSMENT PROCEDURE: AU-2(0).1	104.512(b), IRS-1075. 5.0.5.3#2.1, 5.0.5.3#5, INIST 600-55/55A. AU-2, PISP. 4.5.2	
Assessment Objective		
•	ements as specified in the baseline control and the specific CMS requirements as prescribed in this ampli	iving enhancement to the baseline control
Assessment Methods And Objects		
-	edures addressing auditable events; information system security plan (for list of organization-defined aud	itable events): information system
	ntation; information system audit records; other relevant documents or records.	
AU-2(1) – Enhancement (Moderate)		
Control		
	from multiple components throughout the system into a system-wide (logical or physical) time correlated	audit trail.
Applicability: All	References: ARS: AU-2(1); IRS-1075: 5.6.3.3#2.1	Related Controls:
ASSESSMENT PROCEDURE: AU-2(1).1		
Assessment Objective		
Determine if:		
(i) the organization defines the components of	the information system that generate audit records; and	
Rev. 9	Page 35 of 189	BPSSM Appendix A. Attachment 2

CMS Core Security Requirements for Moderate Impact Level Assessments		
(ii) the information system compiles audit records Assessment Methods And Objects	s from the organization-defined (multiple) components within the information system into a sy	stemwide (logical or physical), time-correlated audit trail.
Examine: Audit and accountability policy; proceed	dures addressing auditable events; information system design documentation; information sys able events; information system audit records; other relevant documents or records.(Optional	
Test: Automated mechanisms implementing a sy		,
AU-2(2) – Enhancement (Moderate)		
Control		
	events to be audited by individual components of the information system.	
Applicability: All	References: ARS: AU-2(2); IRS-1075: 5.6.3.3#2.1	Related Controls:
ASSESSMENT PROCEDURE: AU-2(2).1		
Assessment Objective		
	capability to manage the selection of events to be audited by individual components of the s	ystem.
Assessment Methods And Objects		
documentation; list of organization-defined auditation	dures addressing auditable events; information system design documentation; information systable events; information system audit records; other relevant documents or records.(Optional	
	rmation system auditing for the specified components of the information system.(Optional)	
AU-2(3) – Enhancement (Moderate)		
Control		
Periodically review and update the list of auditab		
Applicability: All	References: ARS: AU-2(3); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2(3)	Related Controls:
ASSESSMENT PROCEDURE: AU-2(3).1		
Assessment Objective		
3 . , ,	s and updates the list of organization-defined auditable events.	
Assessment Methods And Objects		
other relevant documents or records.	dures addressing auditable events; list of organization-defined auditable events; information s	system audit records; information system incident reports;
Interview: Organizational personnel with auditin	a and accountability responsibilities (Ontional)	
AU-2(CMS-1) – Enhancement (Moderate)		
Control		
Enable logging for perimeter devices, including fi	irewalls and routers	
(a) Log packet screening denials originating from		
(b) Packet screening denials originating from true		
(c) User account management,		
(d) Modification of proxy services,		
(e) Application errors, (f) System shutdown and reboot,		
(q) System errors,		
(h) Modification of proxy services, and		
(i) Modification of packet filters.		
Applicability: All	References: ARS: AU-2(CMS-1); HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	Related Controls:
ASSESSMENT PROCEDURE: AU-2(CMS-1).1		
Assessment Objective		
Determine if:		
(i) the organization defines information system a		
	adequate to support after-the-fact investigations of security incidents; and ds for the organization-defined auditable events.	

(iii) the information system generates audit records for the organization-defined auditable events.

Assessment Methods And Objects

Assessment Methods And Objects	
	dures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system
configuration settings and associated documenta	ation; information system audit records; other relevant documents or records to determine if logging-on is enabled for perimeter devices, including
firewalls and routers. This logging will capture the	
(a) Log packet screening denials originating from	
(b) packet screening denials originating from true	ted networks,
(c) user account management,	
(d) modification of proxy services,	
(e) application errors,	
(f) system shutdown and reboot,	
(g) system errors,	
(h) modification of proxy services, and	
(i) modification of packet filters.	
	nd accountability responsibilities to determine if logging-on is enabled for perimeter devices, including firewalls and routers. This logging will capture
the following information:	
(a) Log packet screening denials originating from	
(b) packet screening denials originating from true	ted networks,
(c) user account management,	
(d) modification of proxy services,	
(e) application errors,	
(f) system shutdown and reboot,	
(g) system errors, (h) modification of proxy services, and	
(i) modification of packet filters.	
	rmotion system sudition of experimetion defined systems
	rmation system auditing of organization-defined auditable events.
AU-2(CMS-2) – Enhancement (Moderate)	
Control	
Control Verify that proper logging is enabled in order to a	
Control Verify that proper logging is enabled in order to a Applicability: All	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Control Verify that proper logging is enabled in order to a	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Control Verify that proper logging is enabled in order to a Applicability: All	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events. Image: Control of the organization control o
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proceed	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce- configuration settings and associated documenta	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events. Image: Control of the organization control o
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated documenta activities.	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated documenta activities. Interview: Organizational personnel with account	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce- configuration settings and associated documenta activities. Interview: Organizational personnel with account Test: Automated mechanisms implementing info	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events. udit records for the organization-defined auditable events. information system security plan (for list of organization-defined auditable events); information system security plan (for list of organization-defined auditable events); information system audit records; other relevant documents or records to determine if proper logging is enabled in order to audit administrator at audit and accountability responsibilities to determine if proper logging is enabled in order to audit administrator activities. rmation system auditing of organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce- configuration settings and associated documenta activities. Interview: Organizational personnel with accoun Test: Automated mechanisms implementing info AU-3 – Content of Audit Records (Mode	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events. udit records for the organization-defined auditable events. information system security plan (for list of organization-defined auditable events); information system security plan (for list of organization-defined auditable events); information system audit records; other relevant documents or records to determine if proper logging is enabled in order to audit administrator at audit and accountability responsibilities to determine if proper logging is enabled in order to audit administrator activities. rmation system auditing of organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated documenta activities. Interview: Organizational personnel with accoun Test: Automated mechanisms implementing info AU-3 – Content of Audit Records (Mode Control	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce- configuration settings and associated documenta activities. Interview: Organizational personnel with account Test: Automated mechanisms implementing infor AU-3 – Content of Audit Records (Mode Control Automated mechanisms shall be established to	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce- configuration settings and associated documenta activities. Interview: Organizational personnel with account Test: Automated mechanisms implementing infor AU-3 – Content of Audit Records (Mode Control Automated mechanisms shall be established to	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated documenta activities. Interview: Organizational personnel with accoun Test: Automated mechanisms implementing info AU-3 – Content of Audit Records (Mode Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce- configuration settings and associated documenta activities. Interview: Organizational personnel with accour Test: Automated mechanisms implementing info AU-3 – Content of Audit Records (Mode Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit rec	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce- configuration settings and associated documenta activities. Interview: Organizational personnel with accoun Test: Automated mechanisms implementing info AU-3 – Content of Audit Records (Mode Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit rec- occurred; (iii) type of event; (iv) user/subject ider	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Control Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce- configuration settings and associated documenta activities. Interview: Organizational personnel with accour Test: Automated mechanisms implementing info AU-3 – Content of Audit Records (Mode Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit rec	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.

ASSESSMENT PROCEDURE: AU-3.1			
Assessment Objective			
Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.			
Assessment Methods And Objects			
Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system inc	cident		
reports; other relevant documents or records.			
Test: Automated mechanisms implementing information system auditing of auditable events.(Optional)			
AU-3(1) – Enhancement (Moderate)			
Control			
Provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.			
Applicability: All References: ARS: AU-3(1); NIST 800-53/53A: AU-3(1) Related Controls:			
ASSESSMENT PROCEDURE: AU-3(1).1			
Assessment Objective			
Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.			
Assessment Methods And Objects			
Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; information system security plan; information system			
configuration settings and associated documentation; other relevant documents or records.			
Test: Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject.(Optional)			
AU-3(CMS-1) – Enhancement (Moderate)			
Control			
Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify every 90 days for e	each		
extract that the data is erased or its use is still required.			
Applicability: All References: ARS: AU-3(CMS-1); FISCAM: TAC-4.1; HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.2 Related Controls:			
ASSESSMENT PROCEDURE: AU-3(CMS-1).1			
Assessment Objective			
Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.			
Assessment Methods And Objects			
Examine: Audit and accountability policy; procedures addressing the content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records to determine if the organization records disclosures of sensitive information, including protected health and financial information. The	1		
organization must log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still required.			
Interview: Organizational personnel with account audit and accountability responsibilities to determine if the organization records disclosures of sensitive information, including protected health	and		
financial information. The organization must log information type, date, time, receiving party, and releasing party. Verify every 90 days for each extract that the data is erased or its use is still re			
Test: Automated mechanisms implementing information system auditing of auditable events with organization-defined audit record content.			
AU-4 – Audit Storage Capacity (Moderate)			
Control			
A sufficient amount of information system storage capacity shall be allocated for audit records, and information systems shall be configured to reduce the likelihood of audit records exceeding s	uch		
storage capacity.			
Guidance			
The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements.			
Applicability: All References: ARS: AU-4; IRS-1075: 5.6.3.3#4; NIST 800-53/53A: AU-4; PISP: 4.3.4 Related Controls: AU-2, AU-5, AU-6	, AU-		
ASSESSMENT PROCEDURE: AU-4.1			
	Assessment Objective		
Determine if: (i) the organization defines audit record storage capacity for the information system components that generate audit records; and			
(ii) the organization defines addit record storage capacity for the information system components that generate addit records, and (iii) the organization establishes information system configuration settings to reduce the likelihood of the audit record storage capacity being exceeded.			

Assessment Methods And Objects Examine: Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components generating audit records: list of organization-defined auditable events: information system configuration settings and associated documentation; information system audit records: other relevant documents or records. AU-5 – Response to Audit Processing Failures (Moderate) Control Automated mechanisms shall be established which provide the capability to generate information system alerts for appropriate officials in the event of an audit failure or audit storage capacity being reached and to take appropriate additional actions. Guidance Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Applicability: All References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 Related Controls: AU-4 **ASSESSMENT PROCEDURE: AU-5.1 Assessment Objective** Determine if: (i) the organization defines actions to be taken in the event of an audit processing failure; (ii) the organization defines personnel to be notified in case of an audit processing failure; and (iii) the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure or audit storage capacity being reached. Assessment Methods And Objects Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation: list of personnel to be notified in case of an audit processing failure: information system audit records: other relevant documents or records. Test: Automated mechanisms implementing information system response to audit processing failures.(Optional) AU-5(0) – Enhancement (Moderate) Control Alert appropriate officials and take the following actions in response to an audit failure or audit storage capacity issue: (a) Shutdown the information system, (b) Stop generating audit records, or (c) Overwrite the oldest records, in the case that storage media is unavailable. Applicability: All References: ARS: AU-5(0): NIST 800-53/53A: AU-5: PISP: 4.3.5 **Related Controls:** ASSESSMENT PROCEDURE: AU-5(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for list of actions to be taken by the information system in case of an audit processing failure); information system configuration settings and associated documentation: list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records. AU-6 – Audit Monitoring, Analysis, and Reporting (Moderate) Control Information system audit records shall be reviewed and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and/or suspicious activity. Such activity shall be investigated and reported to appropriate officials, in accordance with current CMS Procedures. Guidance Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. References: ARS: AU-6: FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ij)(D). Applicability: All Related Controls: AU-4, IR-4 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6

ASSESSMENT PROCEDURE: AU-6.1

Assessment Objective

Determine if:

(i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity;

(ii) the organization investigates suspicious activity or suspected violations;

(iii) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and

(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records.

Test: Information system audit monitoring, analysis, and reporting capability.(Optional)

ASSESSMENT PROCEDURE: AU-6.2

Assessment Objective

Determine if the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities.(Optional)

AU-6(1) – Enhancement (Moderate)

Control

Employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Applicability: All	References: ARS: AU-6(1); HIPAA: 164.312(b)	Related Controls:
ASSESSMENT PROCEDURE: AU-6(1) 1		

Assessment Objective

Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Automated mechanisms integrating audit monitoring, analysis, and reporting into an organizational process for investigation and response to suspicious activities.(Optional)

AU-6(2) – Enhancement (Moderate)

Control

Employ automated mechanisms to immediately alert security personnel of the following minimal examples of inappropriate or unusual activities with security implications: threats to infrastructure, systems or assets; threats to CMS sensitive data; and threats to finances, personnel, or property.

Applicability: All	References: ARS: AU-6(2); HIPAA: 164.312(b); NIST 800-53/53A: AU-6(2)	Related Controls:
ASSESSMENT PROCEDURE: AU-6(2).1		

Assessment Objective

Determine if:

(i) the organization defines inappropriate or unusual activities with security implications; and

(ii) the organization employs automated mechanisms to alert security personnel of the occurrence of any organization-defined inappropriate or unusual activities with security implications.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing security alerts.

AU-6(CMS-1) – Enhancement (Moderate)

Control

Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than

once within a twenty-four (24) hour period. Ge	enerate alert notification for technical staff review and assessment.	
Applicability: All	References: ARS: AU-6(CMS-1); FISCAM: TAC-4.2	Related Controls:
ASSESSMENT PROCEDURE: AU-6(CMS-1)).1	
Assessment Objective		
Determine if:		
	s audit records for indications of inappropriate or unusual activity;	
(ii) the organization investigates suspicious activity or suspected violations;		
	opriate/usual activities, suspicious behavior, or suspected violations to approp	priate officials; and
	n response to the reviews/analyses of audit records.	
Assessment Methods And Objects		
records; other relevant documents or records f demand but no less than once within a twenty-	cedures addressing audit monitoring, analysis, and reporting; reports of audit for initialization sequences, log-ons and errors; system processes and perform four (24) hour period. Generate alert notification for technical staff review and the form of the period.	mance; and system resources utilization to determine if anomalies on dassessment.
utilization are recorded to determine anomalies	ble for audit and accountability to determine if initialization sequences, log-on s on demand but no less than once within a twenty-four (24) hour period. Ger	nerate alert notification for technical staff review and assessment.
	alysis, and reporting capability to determine if initialization sequences, log-ons s on demand but no less than once within a twenty-four (24) hour period. Ger	
AU-6(CMS-2) – Enhancement (Moderate)		
Control		
Review network traffic, bandwidth utilization ra Generate alerts for technical staff review and a	ates, alert notifications, and border defense devices to determine anomalies o assessment.	on demand but no less than once within a twenty-four (24) hour period.
Applicability: All	References: ARS: AU-6(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: AU-6(CMS-2)).1	
Assessment Objective		
Determine if the organization regularly reviews	s / analyzes audit records for indications of inappropriate or unusual activity.	
Assessment Methods And Objects		
records; other relevant documents or records f	cedures addressing audit monitoring, analysis, and reporting; reports of audit for initialization sequences, log-ons and errors; system processes and perforn and border defense devices are reviewed to determine anomalies on demand nt.	mance; and system resources utilization to determine if network traffic,
	ble for audit and accountability to determine if network traffic, bandwidth utiliz han once within a twenty-four (24) hour period. Generate alerts for technical s	
Test: Information system audit monitoring, and	alysis, and reporting capability to determine if network traffic, bandwidth utili han once within a twenty-four (24) hour period. Generate alerts for technical s	zation rates, alert notifications, and border defense devices are reviewed to
AU-6(CMS-3) – Enhancement (Moderate)	nan once within a twenty-loar (24) hour pendu. Generate alens for technical s	
Control		
	plations on the information system, report findings to appropriate officials and	take appropriate action
Applicability: All	References: ARS: AU-6(CMS-3); FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3. HIPAA: 164.312(b)	
ASSESSMENT PROCEDURE: AU-6(CMS-3)		
Assessment Objective		
Determine if the organization investigates susp	nicious activity or suspected violations	
Assessment Methods And Objects		
Examine: Audit and accountability policy; proc records; other relevant documents or records f investigates suspicious activity or suspected vi	cedures addressing audit monitoring, analysis, and reporting; reports of audit for initialization sequences, log-ons and errors; system processes and perforn iolations on the information system, and reports findings to appropriate officia ole for audit and accountability to determine if the organization investigates s ses appropriate action.	mance; and system resources utilization to determine if the organization als and takes appropriate action.

Test: Information system au	dit monitoring, analysis, and reporting capability to determine if the organization investigates suspicion	ous activity or suspected violations on the information system, and
AU-6(CMS-4) – Enhancemei	te officials and takes appropriate action.	
Control		
	view audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavio	Dr.
Applicability: All	References: ARS: AU-6(CMS-4): HIPAA: 164.312(b)	Related Controls:
ASSESSMENT PROCEDUR		
Assessment Objective		
•	n employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overal	all process for investigation and response to suspicious activities
ssessment Methods And (
	tability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit finding	as: records of actions taken in records to reviews/analyses of aud
	iments or records for initialization sequences, log-ons and errors; system processes and performance	
	eview audit records once daily for unusual, unexpected, or suspicious behavior.	
	ersonnel responsible for audit and accountability to determine if the organization uses automated utilit	ties to review audit records once daily for unusual, unexpected, or
suspicious behavior.		
	idit monitoring, analysis, and reporting capability to determine if the organization uses automated utilit	ties to review audit records once daily for unusual, unexpected, or
suspicious behavior.		
U-6(CMS-5) – Enhancemei	nt (Moderate)	
Control		
	s on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts	ts have not been created.
pplicability: All	References: ARS: AU-6(CMS-5); FISCAM: TAC-2.1.5; HIPAA: 164.312(b)	Related Controls:
		Neidled Controls.
Assessment Objective		
5	n monitors activities of system administrators.	
Assessment Methods And (•	
	tability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit finding	
	ments or records for initialization sequences, log-ons and errors; system processes and performance	
	nand but at least once every seven (7) days to ensure unauthorized administrator accounts have not ersonnel with audit and accountability responsibilities to determine if administrator groups are inspecte	
5 1	accounts have not been created.	ed on demand but at least once every seven (7) days to ensure
	idit monitoring, analysis, and reporting capability to determine if administrator groups are inspected on	n demand but at least once every seven (7) days to ensure
	accounts have not been created.	in demand but at least once every seven (1) days to ensure
U-6(CMS-6) – Enhancemei		
Control	puster audit records rendemly on demand but at least once avenutbirty (20) days	
	system audit records randomly on demand but at least once every thirty (30) days.	Related Controlo
	References: ARS: AU-6(CMS-6); HIPAA: 164.312(b)	Related Controls:
SSESSMENT PROCEDUR	E: AU-6(CMS-6).1	
ssessment Objective		
	n randomly performs a manual review of automated audit systems to validate the correctness of the a	automated system.
ssessment Methods And (•	
	tability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit finding	
	ments or records for initialization sequences, log-ons and errors; system processes and performance	e; and system resources utilization to determine if the organization
	system audit records randomly on demand but at least once every thirty (30) days.	
	an a second with a well a second a bill the second and bill the standard of the second method is suffering a second	al reviews of system audit records randomly on demand but at leas
	ersonnel with audit and accountability responsibilities to determine if the organization performs manual	
once every thirty (30) days.		· · · · · · · · · · · · · · · · · · ·
	idit monitoring, analysis, and reporting capability to determine if the organization performs manual rev	views of system audit records randomly on demand but at least once

AU-6(FIS-1) – Enhancement (N	Moderate)	
Control	ioderate/	
	oftware and utilities is reviewed by technical management. Systems programmers' activities are monitored	d and reviewed. Inappropriate or unusual activity in using
utilities is investigated.		
pplicability: All	References: FISCAM: TSS-2.2.1, TSS-2.2.2, TSS-2.2.3	Related Controls:
SSESSMENT PROCEDURE:	AU-6(FIS-1).1	
ssessment Objective		
Determine if the organization m	nonitors and reviews system programmers' activities and investigates inappropriate or unusual activities whethe	hen using privileged system software utilities.
ssessment Methods And Ob	viects	
Examine: Documentation supr	porting the supervising and monitoring of systems programmers' activities.	
Examine: Documentation supp	porting their reviews.	
Examine: Documentation supp		
Examine: Pertinent policies an		
	er supervisors to determine their activities related to supervising and monitoring their staff.	
	nent regarding their reviews of privileged system software and utilities usage.	
U-6(IRS-1) – Enhancement (M	Moderate)	
ontrol		
For FTI, all requests for return i	information, including receipt and/or disposal of returns or return information, shall be maintained in a log.	(see IRS Pub. 1075, sect 6.3.1)
pplicability: All	References: IRS-1075: 6.3.1#1	Related Controls:
SSESSMENT PROCEDURE:	AU-6(IRS-1).1	
ssessment Objective		
	naintains a log for all requests for returned FTI, and the log includes receipt and/or disposal of returns (see	IRS Pub. 1075. sect 6.3.1).
ssessment Methods And Ob		
	FTI include receipt and/or disposal or FTI information is returned.	
	zational staff handling FTI to determine is there is an effective log of FTI requests, disposal or returns.	
	d Report Generation (Moderate)	
Control		
	be established and supporting procedures shall be developed, documented, and implemented effectively to	o enable human review of audit information and the
generation of appropriate audit	reports.	
Guidance		
	porting tools support after-the-fact investigations of security incidents without altering original audit records	
pplicability: All	References: ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7	Related Controls: AU-4
SSESSMENT PROCEDURE:	AU-7.1	
ssessment Objective		
Determine if the information sy	stem provides an audit reduction and report generation capability.	
ssessment Methods And Ob	vjects	
Second in methods And Ob		
Examine: Audit and accountab	pility policy; procedures addressing audit reduction and report generation; information system design docur	mentation; audit reduction, review, and reporting tools;
Examine: Audit and accountab information system audit record	ds; other relevant documents or records.	mentation; audit reduction, review, and reporting tools;
Examine: Audit and accountab information system audit record Interview: Organizational perso	ds; other relevant documents or records. connel with information system audit monitoring, analysis, and reporting responsibilities.(Optional)	mentation; audit reduction, review, and reporting tools;
Examine: Audit and accountab information system audit record	ds; other relevant documents or records. connel with information system audit monitoring, analysis, and reporting responsibilities.(Optional)	mentation; audit reduction, review, and reporting tools;
Examine: Audit and accountab information system audit record Interview: Organizational perso Test: Audit reduction and repor	ds; other relevant documents or records. connel with information system audit monitoring, analysis, and reporting responsibilities.(Optional) rt generation capability.	mentation; audit reduction, review, and reporting tools;
Examine: Audit and accountab information system audit record Interview: Organizational person Test: Audit reduction and report U-7(1) – Enhancement (Mode	ds; other relevant documents or records. connel with information system audit monitoring, analysis, and reporting responsibilities.(Optional) rt generation capability.	mentation; audit reduction, review, and reporting tools;
Examine: Audit and accountab information system audit record Interview: Organizational perso Test: Audit reduction and report AU-7(1) – Enhancement (Mode Control	ds; other relevant documents or records. connel with information system audit monitoring, analysis, and reporting responsibilities.(Optional) rt generation capability.	mentation; audit reduction, review, and reporting tools;

ASSESSMENT PROCEDURE: AU-7(1).1		
Assessment Objective		
Determine if the information system provides the	capability to automatically process audit records for events of interest based upon selectable, event cri	teria.
Assessment Methods And Objects		
Examine: Audit and accountability policy; proceed	dures addressing audit reduction and report generation; information system design documentation; infor	mation system configuration settings and
associated documentation; audit reduction, revie	w, and reporting tools; information system audit records; other relevant documents or records.	
Test: Audit reduction and report generation capa	ability.(Optional)	
AU-8 – Time Stamps (Moderate)		
Control		
	n audit record generation. Time stamps of audit records shall be generated using internal system clocks	s that are synchronized system-wide
Guidance		
	ecords are generated using internal system clocks.	
Applicability: All	References: ARS: AU-8; NIST 800-53/53A: AU-8; PISP: 4.3.8	Related Controls:
ASSESSMENT PROCEDURE: AU-8.1		Related Controls.
Assessment Objective	a standar familia 's an Ptananal an and 's a	
Determine if the information system provides tim	e stamps for use in audit record generation.	
Assessment Methods And Objects		
documentation; information system audit records	dures addressing time stamp generation; information system design documentation; information system	configuration settings and associated
Test: Automated mechanisms implementing time		
AU-8(1) – Enhancement (Moderate)		
Control		
Information system clock synchronization occurs		
Applicability: All	References: ARS: AU-8(1); NIST 800-53/53A: AU-8(1)	Related Controls:
ASSESSMENT PROCEDURE: AU-8(1).1		
Assessment Objective		
Determine if:		
	nal clock synchronization for the information system; and	
	ation system clocks periodically in accordance with organization-defined frequency.	
Assessment Methods And Objects		
Examine: Audit and accountability policy; proceed	dures addressing time stamp generation; information system security plan; information system design d	ocumentation; information system
configuration settings and associated documenta		
	rnal information system clock synchronization.(Optional)	
AU-9 – Protection of Audit Information	(Woderate)	
Control		
Audit information and audit tools shall be protect	ed from unauthorized access, modification, and deletion.	
Guidance		
Audit information includes all information (e.g., a	udit records, audit settings, and audit reports) needed to successfully audit information system activity.	
Applicability: All	References: ARS: AU-9; NIST 800-53/53A: AU-9; PISP: 4.3.9	Related Controls:
ASSESSMENT PROCEDURE: AU-9.1		
Assessment Objective		
	it information and audit tools from unauthorized access, modification, and deletion.	
Assessment Methods And Objects		
•	dures addressing protection of audit information; access control policy and procedures; information syst	em design documentation: information system
	ation, information system audit records; audit tools; other relevant documents or records.	
Test: Automated mechanisms implementing auto		
	Page 44 of 189	BPSSM Appendix A Attachment
Rev 9		

AU-10 – Non-Repudiation (Moderate)		
Control		
Non-repudiation mechanisms shall be implemented that enable a later determination whether a given indivi	dual sent a specific message and whether a given individual received a specific message.	
Guidance		
Examples of particular actions taken by individuals include creating information, sending a message, appro message. Non-repudiation protects against later false claims by an individual of not having taken a specific authored a particular document, a sender of not having transmitted a message, a receiver of not having rec services can be used to determine if information originated from an individual, or if an individual took specific received specific information. Non-repudiation services are obtained by employing various techniques or m	action. Non-repudiation protects individuals against later claims by an author of not having eived a message, or a signatory of not having signed a document. Non-repudiation ic actions (e.g., sending an email, signing a contract, approving a procurement request) or echanisms (e.g., digital signatures, digital message receipts, time stamps).	
Applicability: All References: ARS: AU-10; NIST 800-53/53A: AU-10; PIS	P: 4.3.10 Related Controls:	
ASSESSMENT PROCEDURE: AU-10.1		
Assessment Objective		
Determine if the information system provides the capability to determine whether a given individual took a prindicate concurrence or sign a contract] or received a message). Assessment Methods And Objects	articular action (e.g., created information, sent a message, approved information [e.g., to	
Examine: Audit and accountability policy; procedures addressing non-repudiation; information system desi documentation; information system audit records; other relevant documents or records.(Optional) Test: Automated mechanisms implementing non-repudiation capability.(Optional)	gn documentation; information system configuration settings and associated	
AU-11 – Audit Record Retention (Moderate)		
Control		
Audit records shall be retained to provide support for after-the-fact investigations of security incidents, and and Records Administration maintains criteria for record retention across many disciplines and information standards.		
Guidance The organization retains audit records until it is determined that the records are no longer needed for admir and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law audit records relative to such types of actions and standard response processes for each type of action are incident handling and audit record retention.	enforcement actions (CMS sensitive information retention). Standard categorizations of	
Applicability: All References: NIST 800-53/53A: AU-11	Related Controls:	
ASSESSMENT PROCEDURE: AU-11.1		
Assessment Objective Determine if: (i) the organization defines the retention period for audit records generated by the information system; and (ii) the organization retains information system audit records for the organization-defined time period to pro- organizational information retention requirements.	vide support for after-the-fact investigations of security incidents and to meet regulatory and	
Assessment Methods And Objects		
Examine: Audit and accountability policy; procedures addressing audit record retention; organization-define documents or records.		
Interview: Organizational personnel with information system audit record retention responsibilities.(Optional) AU-11(0) – Enhancement (Moderate)		
Control		
Retain audit records for ninety (90) days, and archive old audit records. Retain audit record archives for on	e (1) vear	
Applicability: All References: ARS: AU-11(0); NIST 800-53/53A: AU-11; F		
ASSESSMENT PROCEDURE: AU-11(0).1		
Assessment Objective		
Determine if the organization meets the requirements as specified in the baseline control and the specific C	MS requirements as prescribed in this amplifying ophonoment to the baseline control	

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

Interview: Organizational personnel with information system audit record retention responsibilities.(Optional)

AU-11(PII-1) – Enhancement (Moderate)

Control

Employ mechanisms to facilitate the review of PII disclosure/access records and retain the records for five (5) years or the applicable records control schedule, whichever is longer.

Applicability: All	References: IRS-1075: 3.1#1	Related Controls:

ASSESSMENT PROCEDURE: AU-11(PII-1).1

Assessment Objective

Determine if the organization employs mechanisms to facilitate the review of PII disclosures/access records and retains the records for five (5) years or the applicable records control schedule, whichever is longer.

Assessment Methods And Objects

Examine: PII disclosure/access audit records are retained or a control schedule indicates (5) five years or longer.

AU-11(PII-2) – Enhancement (Moderate)

Control

To support the audit of activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever PII is stored.

Applicability: All References: IRS-1075: 5.6.3.3#5.2 Related Controls: ASSESSMENT PROCEDURE: AU-11(PII-2).1 Ferences: IRS-1075: 5.6.3.3#5.2 Ferences: IRS-1075: 5.6.3.3#5.2

Assessment Objective

Determine if the organization ensures that audit information is archived for six (6) years to enable the recreation of computer related accesses to both the operation system and the application wherever PII is stored.

Assessment Methods And Objects

Examine: PII audit information is retained for (6) six years to enable recreation of computer related access to both the operation system and the application wherever PII is stored.

AU-11(PII-3) – Enhancement (Moderate)

Control

For PII, inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.

Applicability: All	References: IRS-1075: 6.3.5#3
ACCESSION PROCEEDINES AND AVENUAL	

ASSESSMENT PROCEDURE: AU-11(PII-3).1

Assessment Objective

Determine if the organizational PII inspection reports include a record of corrective actions, which is retained for a minimum of three (3) years from the date the inspection was completed.

Assessment Methods And Objects

Examine: PII inspection records to determine inclusion of corrective actions and are retained for a minimum of three (3) years from the inspection completion date.

Related Controls:

Certification, Accreditation, and Security Assessments (CA) - Management

CA-1 – Certification, Accreditation, and Security Assessments Policies and Procedures (Moderate)

Control

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the Business Owner and accredited by the CMS CIO or his/her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the confidentiality, integrity, and availability (CIA) of CMS information and information systems. All C&A and security assessment activities shall be conducted in accordance with current CMS Procedures.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs, MAs, and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and/or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.4.6, Security Accreditation (CA-6).

If the CMS CIO or his/her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his/her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his/her designated representatives.

As part of the system certification and accreditation (C&A), an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, IS Risk Assessment (RA), System Security Plan (SSP), independent system tests and evaluations, the Business Owner and System Developer / Maintainer shall certify that the system meets the security requirements to the extent necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CMS CIO or the Designated Accrediting Authority (DAA).

Guidance

The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security control assessments. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: CA-1; FISCAM: TSP-5.1.2; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075:	Related Controls: CA-6
	5.6.1.4#1.1-2; NIST 800-53/53A: CA-1; PISP: 4.4.1	

ASSESSMENT PROCEDURE: CA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security assessment and certification and accreditation policies and procedures;

(ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review policy and procedures; and

(iv) the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.

Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.(Optional)

ASSESSMENT PROCEDURE: CA-1.2

Assessment Objective

Determine if:

(i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records. **Interview:** Organizational personnel with security assessment and certification and accreditation responsibilities.(Optional)

CA-2 – Security Assessments (Moderate)

Control

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application, and comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Routine assessments shall be conducted every 365 days, in accordance with NIST SP 800-53 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information system.

OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST SP 800-53 A provides guidance on security control assessments to include reuse of existing assessment results.

Applicability: All	References: ARS: CA-2; FISCAM: TSP-5.1.1; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1; NIST 800-53/53A: CA-2; PISP: 4.4.2	Related Controls: CA-4, CA-6, CA-7, CA-7(1), SA-11, SI-2
ASSESSMENT PROCEDURE: CA-2.1		

Assessment Objective

Determine if:

(i) the information system is in the inventory of major information systems; and

(ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security assessment policy; procedures addressing security assessments; information system security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records.

CA-3 – Information System Connections (Moderate)

Control

Management shall authorize in writing through the use of system connection agreements all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system connections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

Guidance

Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST SP 800-47 provides guidance on connecting information systems.

Applicability: All	References: ARS: CA-3; HSPD 7: F(19); NIST 800-53/53A: CA-3; PISP: 4.4.3	Related Controls: SA-9, SC-7
ASSESSMENT PROCEDURE: CA-3.1		

Assessment Objective

Determine if:

(i) the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary);

(ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements;

(iii) the organization monitors/controls the system interconnections on an ongoing basis; and

(iv) information system connection agreements are consistent with NIST SP 800-47.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records.

Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements.(Optional)

CA-3(CMS-1) – Enhancement (Moderate)

Control

 Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

 Applicability: All
 References: ARS: CA-3(CMS-1); FISCAM: TAC-2.1.3; HSPD 7: F(19)
 Related Controls:

ASSESSMENT PROCEDURE: CA-3(CMS-1).1

Assessment Objective

Determine if the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

CA-4 – Security Certification (Moderate)

Control

Business owners shall conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification process shall be integrated into and span across the SDLC. In addition, the Business Owner shall review the certification documentation every 365 days, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his/her designated representative.

Guidance

A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST SP 800-53 A provides guidance on security certification.

Applicability: All	References: ARS: CA-4; FISCAM: TSS-2.2.4; HSPD 7: F(19); IRS-1075: 6.3#1.1-2; NIST 800-	Related Controls: CA-2, CA-6, CA-7, SA-
	53/53A: CA-4; PISP: 4.4.4	11, SI-2

ASSESSMENT PROCEDURE: CA-4.1

Assessment Objective

Determine if:

(i) the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and

(ii) the organization employs a security certification process in accordance with OMB policy and NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.

Interview: Organizational personnel with security certification responsibilities.(Optional)

CA-4(1) – Enhancement (Moderate)

Control

Employ an independent certification agent or certification team to conduct an assessment of the information system security controls.

Guidance

An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization and/or management chain of the system owner or authorizing official, independence in the certification process can be accomplished by individuals that are in the developmental, operational, and/or management chain of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circums

Applicability: All	References: ARS: CA-4(1); HSPD 7: F(19); NIST 800-53/53A: CA-4(1)	Related Controls: AC-9
ASSESSMENT PROCEDURE: CA-4(1).1		

Assessment Objective

Determine if the organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; security accreditation package (including information system security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.

CA-4(CMS-1) – Enhancement (Moderate)

Control

Document the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures.

Applicability: All	References: ARS: CA-4(CMS-1); HSPD 7: F(19), G(24)	Related Controls:
ASSESSMENT PROCEDURE: CA-4(CMS-1).1		

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.

Interview: Organizational personnel with security certification responsibilities to determine the risk and safeguards of the system according to the CMS Information Security Risk Assessment (RA) Procedures are documented.

CA-5 – Plan of Action and Milestones (POA&M) (Moderate)

Control

A POA&M shall be developed, implemented, and updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M shall document the planned, implemented, and evaluated corrective actions to repair deficiencies discovered during the security control assessment, and to reduce or eliminate any known vulnerability in the information system.

Personnel shall be designated to assign, track, and update risk mitigation efforts. Designated personnel shall define and authorize corrective action plans, and monitor corrective action progress.

Guidance

The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems. NIST SP 800-30 provides guidance on risk mitigation.

pplicability: All		References: ARS: CA-5; FISCAM: TSP-5.2; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4; NIST 8(53/53A: CA-5; PISP: 4.4.5	0- Related Controls: CA-7
SSESSMENT PROCEDURE: CA-5.1			
ssessment Objective			
Determine if:			
		organization-defined frequency, a plan of action and milestones for the information system; and	
		he planned, implemented, and evaluated remedial actions by the organization to correct any deficier	cies noted during the assessment of the securit
controls and to reduce or eliminate kno		abilities in the information system.	
ssessment Methods And Objects			
assessment evidence; plan of action ar	and milestor	rocedures addressing plan of action and milestones; information system security plan; security asse nes; other relevant documents or records.	ssment plan; security assessment report;
	with plan of	action and milestones development and implementation responsibilities.(Optional)	
A-5(0) – Enhancement (Moderate)			
Control			
		es (POA&M) for any documented information system security finding within thirty (30) days of the fir ate the POA&M monthly until all the findings are resolved.	al results for every internal / external audit /
pplicability: All		References: ARS: CA-5(0); HSPD 7: F(19), G(24); NIST 800-53/53A: CA-5; PISP: 4.4.5	Related Controls:
SSESSMENT PROCEDURE: CA-5(0			
ssessment Objective	. ,		
	he requirem	ents as specified in the baseline control and the specific CMS requirements as prescribed in this am	olifving enhancement to the baseline control.
ssessment Methods And Objects	•		
		nd procedures; information system security plan (for organization-defined frequency of plan of action	and milestones updates): security assessment
		dence; plan of action and milestones; other relevant documents or records.	
Interview: Organizational personnel wi	with plan of	action and milestones development and implementation responsibilities.(Optional)	
A-6 – Security Accreditation (N	Moderate		
Control			
Explicit authorization to operate the info	nformation s	ystem shall be received from the CMS CIO or his/her designated representative prior to the system by	eing placed into operations. If the authorization
		zation shall be granted based on the designated security category of the information system. An ex	plicit corrective action plan shall be developed,
		thorizing official. Re-authorization shall be obtained prior to continued operation:	
4.4.6.1. At least every three (3) years;			
4.4.6.2. When substantial changes are			
4.4.6.4. When changes occur to author		he need to process data of a higher sensitivity;	
		violation which raises questions about the validity of an earlier certification; and	
4.4.6.6. Prior to expiration of a previous	,		
Buidance			
OMB Circular A-130, Appendix III, esta	tablishes po	licy for security accreditations of federal information systems. The organization assesses the securit	controls employed within the information
system before and in support of the sec	ecurity accre	editation. Security assessments conducted in support of security accreditations are called security ca	ertifications. The security accreditation of an
		the employment of a comprehensive continuous monitoring process (the fourth and final phase of	
		backage (i.e., the system security plan, the security assessment report, and the plan of action and m	
		on system owner with an up-to-date status of the security state of the information system. To reduce	
		the set of the ongoing continuous monitoring process to the maximum extent possible as the	basis for rendering a reaccreditation decision.
pplicability: All		ty certification and accreditation of information systems. References: ARS: CA-6; FISCAM: TSP-5.1.3, TSP-5.2; HSPD 7: F(19); NIST 800-53/53A: CA-6;	Related Controls: CA-1, CA-2, CA-4, CA
ppilcapility. All			
		PISP: 4.4.6	
SSESSMENT PROCEDURE: CA-6.1			

	e information system for processing before operations and updates the authorization in accorda	ance with organization-defined frequency, at least every
three (3) years; (ii) a senior organizational official signs and appro	oves the security accreditation:	
	by the organization is consistent with NIST SP 800-37; and	
	nen there is a significant change to the information system.	
Assessment Methods And Objects		
	procedures addressing security accreditation; NIST SP 800-37; security accreditation package s; authorization statement); other relevant documents or records.	(including information system security plan; security
Interview: Organizational personnel with security	y accreditation responsibilities.(Optional)	
CA-6(0) – Enhancement (Moderate)		
Control		
Information systems can only be accredited for a	maximum period of three (3) years, after which the information system must be re-accredited.	
Applicability: All	References: ARS: CA-6(0); HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6	Related Controls:
ASSESSMENT PROCEDURE: CA-6(0).1		
Assessment Objective		
Determine if the organization meets the requirem	nents as specified in the baseline control and the specific CMS requirements as prescribed in the	his amplifying enhancement to the baseline control.
Assessment Methods And Objects		
	procedures addressing security accreditation; NIST SP 800-37; security accreditation package	(including information system security plan; security
· · · ·	s; authorization statement); other relevant documents or records.	
CA-7 – Continuous Monitoring (Modera	te)	
Control		
	all be monitored on an on-going basis. Selection criteria for control monitoring shall be established	shed and a subset of the security controls employed
within information systems shall be selected for o	continuous monitoring purposes.	
security controls, and status reporting. The organ accordance with OMB policy, the organization as FIPS 199 security categorization of the information assurance (or grounds for confidence) that the or- criteria and subsequently selects a subset of the ensure adequate coverage is achieved. Those sec- once during the information system's three-year assessment requirement (see CA-2). This control is closely related to and mutually sup ongoing updates to the information system secur A rigorous and well executed continuous monitor the continuous monitoring process. NIST SP 800	ation management and control of information system components, security impact analyses of nization assesses all security controls in an information system during the initial security accred sessess a subset of the controls annually during continuous monitoring. The selection of an app on system; (ii) the specific security controls selected and employed by the organization to prote rganization must have in determining the effectiveness of the security controls in the information security controls employed within the information system for assessment. The organization als ecurity controls that are volatile or critical to protecting the information system are assessed at accreditation cycle. The organization can use the current year's assessment results obtained of poportive of the activities required in monitoring configuration changes to the information system ity plan, the security assessment report, and the plan of action and milestones—the three prin- ing process significantly reduces the level of effort required for the reaccreditation of the inform b D D D D D D D D D D	ditation. Subsequent to the initial accreditation and in propriate subset of security controls is based on: (i) the ect the information system; and (iii) the level of on system. The organization establishes the selection so establishes the schedule for control monitoring to least annually. All other controls are assessed at least during continuous monitoring to meet the annual FISMA a. An effective continuous monitoring program results in ciple documents in the security accreditation package. nation system. NIST SP 800-37 provides guidance on
Applicability: All	References: ARS: CA-7; HSPD 7: F(19); NIST 800-53/53A: CA-7; PISP: 4.4.7	Related Controls: CA-2, CA-4, CA-5, CA- 6, CM-4, SI-2
ASSESSMENT PROCEDURE: CA-7.1		
 (ii) the organization employs a security control m Assessment Methods And Objects Examine: Certification and accreditation policy; p 	in the information system on an ongoing basis; and onitoring process consistent with NIST SP 800-37 and 800-53A. procedures addressing continuous monitoring of information system security controls; NIST SF and milestones; information system monitoring records; security impact analyses; status report ious monitoring responsibilities.(Optional)	

ASSESSMENT PROCEDURE: CA	7.2	
Assessment Objective	·	
Determine if:		
(i) the organization conducts securi	ty impact analyses on changes to the information system;	
(ii) the organization documents and	I reports changes to or deficiencies in the security controls employed in the information system; and	
	nents to the information system security plan and plan of action and milestones, as appropriate, based	on the activities associated with continuous monitoring of the
security controls.		
Assessment Methods And Object		
	tation policy; procedures addressing continuous monitoring of information system security controls; info	
	mation system monitoring records; security impact analyses; status reports; other relevant documents	or records.
	el with continuous monitoring responsibilities.(Optional)	
CA-7(1) – Enhancement (Moderat	e)	
Control		
information system on an on-going	n agents or teams is not required but, if the organization uses an independent certification agent or cert basis, this can be used to satisfy ST&E requirements.	tification team to monitor the security controls in the
Guidance		
The use of independent certification satisfy ST&E requirements.	n agents or teams is not required but, if used by the organization to monitor the security controls in the	information system on an on-going basis, this can be used to
Applicability: All	References: ARS: CA-7(1); HSPD 7: F(19); NIST 800-53/53A: CA-7(1)	Related Controls: AC-9, CA-2
ASSESSMENT PROCEDURE: CA	-7(1).1	
Assessment Objective		
-	bys an independent certification agent or certification team to monitor the security controls in the inform	nation system on an ongoing basis.
Assessment Methods And Object		
	tation policy; procedures addressing continuous monitoring of information system security controls; info	ormation system security plan: security assessment report:
	mation system monitoring records; security impact analyses; status reports; other relevant documents	
	el with continuous monitoring responsibilities.(Optional)	
CA-7(CMS-1) - Enhancement (Mo	derate)	
Control		
Continuous monitoring activities ind	clude:	
(a) Configuration management;		
(b) Control of information system co		
(c) Security impact analyses of cha		
(d) On-going assessment of securit	y controls; and	
(e) Status reporting.		Delete d Oscatas la
	References: ARS: CA-7(CMS-1); HSPD 7: F(19)	Related Controls:
ASSESSMENT PROCEDURE: CA	//(CMS-1).1	
Assessment Objective		
Determine if:		
0	curity controls in the information system on an ongoing basis; and	
	urity control monitoring process consistent with NIST SP 800-37 and 800-53A.	
Assessment Methods And Object		
	tation policy; procedures addressing continuous monitoring of information system security controls; NIS	
	lan of action and milestones; information system monitoring records; security impact analyses; status r	reports; other relevant documents or records to determine
continuous monitoring activities inc	lude:	
(a) Configuration management;(b) Control of information system ca	amoonents:	
(c) Security impact analyses of cha		

- (c) Security impact analyses of changes to the system; (d) On-going assessment of security controls; and

(e) Status reporting.

Interview: Organizational personnel with continuous monitoring responsibilities to determine continuous monitoring activities include:

(a) Configuration management;

(b) Control of information system components;(c) Security impact analyses of changes to the system;

(d) On-going assessment of security controls; and

(e) Status reporting.

Configuration Management (CM) - Operational

CM-1 – Configuration Management Policy and Procedures (Moderate)

Control

A CM process that includes the approval, testing, implementation, and documentation of changes shall be developed, documented, and implemented effectively to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with the organization's information technology architecture plans. Formally documented CM roles, responsibilities, procedures, and documentation shall be in place.

Guidance

The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

J ,	· · · · · · · · · · · · · · · · · · ·	
Applicability: All	References: ARS: CM-1; FISCAM: TCC-2.1.9, TCC-3.2.1, TCC-3.2.2, TCC-3.3.1, TSS-3.1.1, TSS-	Related Controls:
	3.1.2, TSS-3.1.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-1; PISP: 4.5.1	

ASSESSMENT PROCEDURE: CM-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents configuration management policy and procedures;

(ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization;

- (iii) responsible parties within the organization periodically review configuration management policy and procedures; and
- (iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.

Interview: Organizational personnel with configuration management and control responsibilities.(Optional)

ASSESSMENT PROCEDURE: CM-1.2

Assessment Objective

Determine if:

(i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.

Interview: Organizational personnel with configuration management and control responsibilities.(Optional)

CM-2 – Baseline Configuration (Moderate)

Control

A baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system shall be developed and documented. Procedures shall be developed, documented, and implemented effectively to maintain the baseline configuration. The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture.

Guidance

This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture.

Applicability: All	References: ARS: CM-2; HIPAA: 164.310(b); NIST 800-53/53A: CM-2; PISP: 4.5.2	Related Controls: CM-6, CM-8
ASSESSMENT PROCEDURE: CM-2.1		
Assessment Objective		

Assessment Objective

Determine if:

(i) the organization develops, documents, and maintains a baseline configuration of the information system;

(ii) the baseline configuration shows relationship	os among information system components and is consistent with the Federal Enterprise Ar	rchitecture
	nization with a well-defined and documented specification to which the information system	
	the baseline configuration, in support of mission needs/objectives.	
Assessment Methods And Objects		
Examine: Configuration management policy; pro	ocedures addressing the baseline configuration of the information system; Federal Enterp	rise Architecture documentation; information system design
	and configuration documentation; other relevant documents or records.	
CM-2(1) – Enhancement (Moderate)		
Control		
Update the baseline configuration of the informa	ation system as an integral part of information system component installations.	
Applicability: All	References: ARS: CM-2(1); NIST 800-53/53A: CM-2(1)	Related Controls:
ASSESSMENT PROCEDURE: CM-2(1).1		
Assessment Objective		
Determine if:		
	pdates to the baseline configuration and instances that trigger configuration updates; and	
	uration of the information system as an integral part of information system component insta	allations.
Assessment Methods And Objects		
	rocedures addressing the baseline configuration of the information system; information sys	stem architecture and configuration documentation; other
relevant documents or records.		
CM-2(CMS-1) – Enhancement (Moderate)		
Control		
	configuration and any other system-related operations or security documentation at least o	nce every year, and while planning major system changes /
upgrades.	<u>+</u>	
Applicability: All	References: ARS: CM-2(CMS-1); FISCAM: TSS-3.2.6	Related Controls:
ASSESSMENT PROCEDURE: CM-2(CMS-1).1	1	
Assessment Objective		
	ents, and maintains a baseline configuration of the information system.	
Assessment Methods And Objects		
Examine: Configuration management policy; pro	ocedures addressing the baseline configuration of the information system; Federal Enterp	prise Architecture documentation; information system design
	and configuration documentation; other relevant documents or records to determine the b ved and updated at least once every year, and while planning major system changes / upg	
	ved and updated at least once every year, and while planning major system changes / upd	
Interview Organizational paraannal with config		
	uration management responsibilities to determine the baseline configuration and any othe	
reviewed and updated at least once every year,		
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate)	uration management responsibilities to determine the baseline configuration and any othe	
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control	juration management responsibilities to determine the baseline configuration and any othe and while planning major system changes / upgrades.	
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of the information system	juration management responsibilities to determine the baseline configuration and any othe and while planning major system changes / upgrades.	r system-related operations or security documentation are
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of the information system Applicability: All	and while planning major system changes / upgrades.	
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of the information system Applicability: All ASSESSMENT PROCEDURE: CM-2(CMS-2).1	and while planning major system changes / upgrades.	r system-related operations or security documentation are
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of the information system Applicability: All ASSESSMENT PROCEDURE: CM-2(CMS-2).1 Assessment Objective	and while planning major system changes / upgrades. em's operations and security documentation. References: ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6 1	r system-related operations or security documentation are Related Controls:
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of the information system Applicability: All ASSESSMENT PROCEDURE: CM-2(CMS-2).1 Assessment Objective Determine if the organization updates the baseling	and while planning major system changes / upgrades.	r system-related operations or security documentation are Related Controls:
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of the information system Applicability: All ASSESSMENT PROCEDURE: CM-2(CMS-2).1 Assessment Objective Determine if the organization updates the baselin Assessment Methods And Objects	and while planning major system changes / upgrades. em's operations and security documentation. References: ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6 1 ine configuration of the information system as an integral part of information system compo	r system-related operations or security documentation are Related Controls: onent installations.
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of the information system Applicability: All ASSESSMENT PROCEDURE: CM-2(CMS-2).1 Assessment Objective Determine if the organization updates the baselin Assessment Methods And Objects Examine: Configuration management policy; pro-	and while planning major system changes / upgrades. em's operations and security documentation. References: ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6 1	Pr system-related operations or security documentation are Related Controls: onent installations. prise Architecture documentation; information system design
reviewed and updated at least once every year, CM-2(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of the information system Applicability: All ASSESSMENT PROCEDURE: CM-2(CMS-2).1 Assessment Objective Determine if the organization updates the baselin Assessment Methods And Objects Examine: Configuration management policy; prodocumentation; information system architecture security documentation is maintained.	and while planning major system changes / upgrades. em's operations and security documentation. References: ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6 1 ine configuration of the information system as an integral part of information system comporcedures addressing the baseline configuration of the information system; Federal Enterp	Pr system-related operations or security documentation are Related Controls: Onent installations. Prise Architecture documentation; information system design pdated list of the information system's operations and

CM-3 – Configuration Change Control (Moderate)

Control

Change control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to control changes to the information system. Change request forms shall be used to document requests with related approvals. Change requests shall be approved by the Business Owner, or his/her designated representative, and other appropriate organization officials including, but not limited to, the system maintainer and information system support staff.

Test plans shall be developed and approved for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control) and shall include appropriate consideration of security. Test results shall be documented and appropriate responsive actions shall be taken based on the results.

Emergency changes for the CMS information system shall be documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration shall be documented appropriately and approved, and responsible personnel shall be notified for security analysis and follow-up.

Guidance

The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system.

Applicability: All	References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC-	Related Controls: CM-4, CM-6, SI-2
	2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075:	
	5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3	

ASSESSMENT PROCEDURE: CM-3.1

Assessment Objective

Determine if:

(i) the organization authorizes, documents, and controls changes to the information system;

(ii) the organization manages configuration changes to the information system using an organizationally approved process;

(iii) the organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws; and

(iv) the organization audits activities associated with configuration changes to the information system.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing information system configuration change control; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

CM-3(FIS-1) – Enhancement (Moderate)

Control

Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.

Applicability: All	References: FISCAM: TCC-2.1.11	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-1).1		

Accessment Objective

Assessment Objective

Determine if the organization reviews production program changes for access and change control compliance.

Assessment Methods And Objects

Examine: Documentation of management or security administrator reviews.

Examine: Pertinent policies and procedures.

Interview: Information system management or security administrators.

CM-3(FIS-2) – Enhancement (Moderate)

Control

Migration of tested and approved system software to production use is performed by an independent library control group.

Applicability: All	References: FISCAM: TSS-3.2.2	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-2).1		

Assessment Objective

Determine if the organizational independent library control group migrates tested and approved software into production.

Assessment Methods And Objects		
Assessment Methods And Objects		
Examine: Pertinent policies and procedures. Examine: Supporting documentation for some	system software migrations	
	s, and library control personnel, and determine who migrates approved system software to production lib	raries.
CM-3(FIS-3) – Enhancement (Moderate)		
Control		
	ninimize the impact on data processing and advance notice is given to system users.	
Applicability: All	References: FISCAM: TSS-3.2.1	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-3).1	·	
Assessment Objective		
-	schedules to system users which minimize system software installation impacts.	
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Recent installations and determine w	hether scheduling and advance notification did occur.	
Interview: Management and systems program	ners about scheduling and giving advance notices when system software is installed.	
CM-3(FIS-4) – Enhancement (Moderate)		
Control		
Outdated versions of system software are remo	ved from production libraries.	
Applicability: All	References: FISCAM: TSS-3.2.3	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-4).1		
Assessment Objective		
Determine if the organization removes outdated	l versions of system software from the production libraries.	
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
	noval of outdated versions from production libraries.	
	s, and library control personnel, and determine whether outdated versions are removed from production I	ibraries.
CM-4 – Monitoring Configuration Change	ges (Moderate)	
Control		
	in place and supporting procedures shall be developed, documented, and implemented effectively to me	
	hall be conducted after system changes are made to determine the IS-related effects of the changes. A	ctivities associated with configuration changes
to the information system shall be audited.		
Guidance		
	the change approval process, the organization analyzes changes to the information system for potential	
	ns), the organization checks the security features to verify that the features are still functioning properly. In the security is the security features and conducting security impact analyses are important elements.	
security controls in the information system.		with regard to the origoing assessment of
Applicability: All	References: ARS: CM-4; FISCAM: TCC-2.1.11, TCC-2.2.2, TCC-2.3.1, TCC-3.1, TSS-3.1.4; NIST 800-53/53A: CM-4; PISP: 4.5.4	Related Controls: CA-7, CM-3
ASSESSMENT PROCEDURE: CM-4.1	· · · · · ·	
Assessment Objective		
Determine if:		
(i) the organization identifies the types of inform	ation system changes to be monitored;	
(ii) the organization monitors changes to the info		
(iii) the organization conducts security impact a	nalyses to assess the effects of the information system changes.	
Assessment Methods And Objects		
	ocedures addressing the monitoring of configuration changes to the information system; information systation system audit records; other relevant documents or records.	tem architecture and configuration
Rev. 9	Page 58 of 189	BPSSM Appendix A. Attachment 2

CM-4(CMS-1) – Enhancement (Moderate)		
Control		
	nstallation of information system components in the appropriate system document	
Applicability: All	References: ARS: CM-4(CMS-1); FISCAM: TCC-2.1.10, TCC-2.2.2, TCC-2.3.1,	, TCC-3.1, TSS-3.1.4 Related Controls:
ASSESSMENT PROCEDURE: CM-4(CMS-1).	1	
Assessment Objective		
Determine if:		
(i) the organization identifies the types of information		
(ii) the organization monitors changes to the info		
	alyses to assess the effects of the information system changes.	
Assessment Methods And Objects		
documentation; change control records; informa system components is recorded in the appropria		when changes to the system occur, the installation of information
	ation system monitoring responsibilities to determine that when changes to the sy	ystem occur, the installation of information system components is
recorded in the appropriate system documentati	on resource(s).	
CM-4(FIS-1) – Enhancement (Moderate)		
Control		
Library management software is used to: (1) ma control concurrent updates.	intain program version numbers, (2) maintain creation/date information for product	tion modules, (3) maintain copies of previous versions, and (4)
Applicability: All	References: FISCAM: TCC-3.1	Related Controls:
ASSESSMENT PROCEDURE: CM-4(FIS-1).1		
Assessment Objective		
	gement software to: (1) maintain program version numbers, (2) maintain creation/d dates.	date information for production modules, (3) maintain copies of
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
	he library and assess compliance with prescribed procedures.	
Interview: Personnel responsible for library con		
Test: Verify how many prior versions of software	modules are maintained.	
CM-4(FIS-2) – Enhancement (Moderate)		
Control		
Before and after images of program code are ma	aintained and compared to ensure that only approved changes are made.	
Applicability: All	References: FISCAM: TCC-3.3.2	Related Controls:
ASSESSMENT PROCEDURE: CM-4(FIS-2).1		
Assessment Objective		
	oved program changes are made by maintaining and comparing before and after p	program code images.
Assessment Methods And Objects		
-	examine related documentation to verify that before and after images were compar	ared.
Examine: Pertinent policies and procedures.	,	
Interview: Application programmers, if available	ı	
CM-5 – Access Restrictions for Change	(Moderate)	
Control		
Access control change mechanisms shall be in p	place and supporting procedures shall be developed, documented, and implement ed with changes to the information system. Records reflecting all such changes sl	
¥		

	software, and/or firmware components of the information system can have significant effects on the over to information system components for purposes of initiating changes, including upgrades, and modific	
Applicability: All	References: ARS: CM-5; FISCAM: TCC-3.2.3, TCC-3.3.1, TSS-1.2.1, TSS-1.2.2, TSS-3.1.4, TSS- 3.2.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-5; PISP: 4.5.5	Related Controls:
ASSESSMENT PROCEDURE: CM-5.1		
Assessment Objective		
Determine if:		
(ii) the organization approves individual access p	nd authorized personnel permitted to access the information system for the express purpose of initiating privileges and enforces physical and logical access restrictions associated with changes to the information and reflection all such abar set to the information purpose and the information of the set of the set of the information of the set of the information of the set of the information of the set of the set of the information of the set of	3
Assessment Methods And Objects	ews records reflecting all such changes to the information system.	
	ocedures addressing access restrictions for changes to the information system; information system arch	itecture and configuration documentation:
change control records; information system audi		
	estrictions for changes to the information system.(Optional)	
CM-6 – Configuration Settings (Modera		
Control		
Procedures shall be developed, documented, ar configuration settings for information technology	nd implemented effectively to configure and benchmark information technology products in accordance v products employed within the information system shall be established. The security settings of information system operational requirements, documented, and enforced in all components of the information system.	tion technology products shall be configured t
Guidance		
settings in accordance with organizational policie	meters of the information technology products that compose the information system. Organizations mon es and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements f	or federal information systems. NIST SP 800-
Applicability: All	onfiguration settings for information technology products employed in organizational information systems References: ARS: CM-6; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6; PISP: 4.5.6	Related Controls: CM-2, CM-3, CM-8, SI-
	References. ANS. CM-0, INS-1073. 3.0.2.3#1, NOT 000-33/33A. CM-0, 1101 . 4.3.0	
ASSESSMENT PROCEDURE: CM-6.1		
Assessment Objective		
Determine if:		
	guration settings for information technology products employed within the information system;	
	igs of information technology products to the most restrictive mode consistent with operational requirem	ents;
(iii) the organization documents the configuration		
(iv) the organization enforces the configuration s	ettings in all components of the information system.	
Assessment Methods And Objects		
Examine: Configuration management policy; pro SP 800-70; other relevant documents or records	ocedures addressing configuration settings for the information system; information system configuration	settings and associated documentation; NIST
Test: Information system configuration settings.		
CM-6(CMS-1) – Enhancement (Moderate)		
Control		
Configure the information system to provide only application functionality.	v essential capabilities and services by disabling all system services, ports, and network protocols that a	re not explicitly required for system and
Applicability: All	References: ARS: CM-6(CMS-1); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: CM-6(CMS-1).	1	
Assessment Objective		
Determine if:		
(i) the organization establishes mandatory config	guration settings for information technology products employed within the information system;	
	igs of information technology products to the most restrictive mode consistent with operational requirem	ents; and
(iii) the organization documents the configuration	n settings.	

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST SP 800-70; other relevant documents or records to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

Interview: Organizational personnel with configuration management responsibilities to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

Test: Information system to determine the information system is configured to provide only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system and application functionality.

CM-7 – Least Functionality (Moderate)

Control

Information systems shall be configured to provide only essential capabilities. The functions and services provided by CMS information systems shall be reviewed carefully to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol [VoIP], Instant Messaging [IM], File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP], file sharing). The use of those functions, ports, protocols, and/or services shall be prohibited and/or restricted.

Guidance

Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

 Applicability: All
 References: ARS: CM-7; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7; PISP: 4.5.7
 Related Controls:

 ASSESSMENT PROCEDURE: CM-7.1
 Assessment Objective
 Ferences: ARS: CM-7; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7; PISP: 4.5.7
 Related Controls:

Determine if:

(i) the organization identifies prohibited or restricted functions, ports, protocols, and services for the information system;

(ii) the organization configures the information system to provide only essential capabilities; and

(iii) the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for disabling or restriction of functions, ports, protocols, and services.

CM-7(0) – Enhancement (Moderate)

Control

Configure the information system specifically to only essential capabilities and services by disabling all system services, ports, and network protocols that are not explicitly required for system / application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.

Applicability: All	References: ARS: CM-7(0); IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-7; PISP: 4.5.7	Related Controls:
ASSESSMENT PROCEDURE: CM-7(0).1	-	

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan (for list of organization-defined prohibited or restricted functions, ports, protocols, and services for the information system); information system configuration settings and associated documentation; other relevant documents or records. **Test:** Information system configuration settings.

CM-8 – Information System Component Inventory (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to document and maintain a current inventory of the information system's constituent components and relevant ownership information. The inventory of information system components shall include manufacturer, model / type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership.

Guidance		
The inventory of information system component	vel of granularity for the information system components included in the inventory that are subject to mar ts includes any information determined to be necessary by the organization to achieve effective property ation, system/component owner). The component inventory is consistent with the accreditation boundary	accountability (e.g., manufacturer, model
Applicability: All	References: ARS: CM-8; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8; PISP: 4.5.8	Related Controls: CM-2, CM-6
ASSESSMENT PROCEDURE: CM-8.1		
Assessment Objective		
Determine if:		
(i) the organization develops, documents, and r	naintains a current inventory of the components of the information system; and	
(ii) the inventory of information system component	ents includes any information determined to be necessary by the organization to achieve effective prope	rty accountability.
Assessment Methods And Objects		
Examine: Configuration management policy; p	ocedures addressing information system component inventory; information system inventory records; of	her relevant documents or records.
CM-8(1) – Enhancement (Moderate)		
Control		
Update the information system component inve	ntory as an integral part of component installations.	
Applicability: All	References: ARS: CM-8(1); HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8(1)	Related Controls:
ASSESSMENT PROCEDURE: CM-8(1).1		
Assessment Objective		
Determine if the organization updates the inven	tory of information system components as an integral part of component installations.	
Assessment Methods And Objects		
Examine: Configuration management policy; polocy documents or records.	rocedures addressing information system component inventory; information system inventory records; co	omponent installation records; other relevant
Interview: Organizational personnel with inform	nation system installation and inventory responsibilities (Ontional)	

Interview: Organizational personnel with information system installation and inventory responsibilities.(Optional)

Contingency Planning (CP) – Operational

CP-1 – Contingency Planning Policy and Procedures (Moderate)

Control

All major CMS information systems shall be covered by a CP that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

Guidance

The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-34 provides guidance on contingency planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: 1075: 5.6.2.2	ARS: CP-1; FISCAM: TSC-2.2.2; HIPAA: 164.308(a)(7)(i), 164 #1.1; NIST 800-53/53A: CP-1; PISP: 4.6.1	1.308(a)(7)(ii)(B); IRS-	Related Controls:

ASSESSMENT PROCEDURE: CP-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents contingency planning policy and procedures;

(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and

(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: CP-1.2

Assessment Objective

Determine if:

(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

CP-2 – Contingency Plan (Moderate)

Control

All major CMS information systems shall be covered by a CP, relative to the system security level, providing continuity of support in the event of a disruption of service. A CP for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A CP for the information system shall be consistent with NIST SP 800-34. Designated officials within the organization shall review and approve the CP and distribute copies of the plan to key contingency personnel.

Guidance

Contingency Plans consist of all components listed in the CMS Business Partners system Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.

Applicability: All	References: ARS: CP-2; FISCAM: TSC-1.1, TSC-1.2, TSC-1.3, TSC-2.1.2, TSC-3.1.1, TSC-3.1.2,	Related Controls:
	TSC-3.1.3, TSC-3.1.4, TSC-3.2.3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i);	
	IRS-1075: 5.6.2.2#1.3; NIST 800-53/53A: CP-2; PISP: 4.6.2	
	*	*

ASSESSMENT PROCEDURE: CP-2.1

Assessment Objective

I wa i a i i i i i i			
(i) the organization develops and documents a			
(ii) the contingency plan is consistent with NIST SP 800-34; (iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption			
or failure;			
(iv) the contingency plan is reviewed and appro			
(v) the organization disseminates the contingen	cy plan to key contingency personnel.		
Assessment Methods And Objects			
	ures addressing contingency operations for the information system	stem; NIST SP 800-34; contingency plan; o	ther relevant documents or records.
ASSESSMENT PROCEDURE: CP-2.2			
Assessment Objective			
	e key operating elements within the organization understand the	e contingency plan and are ready to impler	nent the plan.
Assessment Methods And Objects			
	gency planning and plan implementation responsibilities.		
CP-2(1) – Enhancement (Moderate)			
Control			
(COOP), Business Recovery Plan, and Incident	an (CP) with parties responsible for related plans, such as the Response Plan.	Business Continuity Plan, Disaster Recove	ry Plan, Continuity of Operations Plan
Guidance			
	ntinuity Plan, Disaster Recovery Plan, Continuity of Operation		
Applicability: All	References: ARS: CP-2(1); FISCAM: TSC-3.1.3; HIPAA: 1 800-53/53A: CP-2(1)	64.308(a)(7)(ii)(E); HSPD 7: G(22)(i); NIST	Related Controls:
ASSESSMENT PROCEDURE: CP-2(1).1			
Assessment Objective			
Determine if the organization coordinates the co Plan, Incident Response Plan, Emergency Action	ontingency plan with other related plans (e.g., Business Contir on Plan).	uity Plan, Disaster Recovery Plan, Continu	ity of Operations Plan, Business Recovery
Assessment Methods And Objects			
	ures addressing contingency operations for the information system of planning and plan implementation responsibilities and r		other relevant documents or records.
CP-2(2) – Enhancement (Moderate)		· · ·	
Control			
	apacity for information processing, telecommunications, and er	vironmental support exists during crisis site	uations.
Applicability: All	References: ARS: CP-2(2); HSPD 7: G(22)(i)		Related Controls:
ASSESSMENT PROCEDURE: CP-2(2).1			
Assessment Objective			
	planning so that necessary capacity for information processing	g, telecommunications, and environmental	support exists during crisis situations.
Assessment Methods And Objects		-	
	ures addressing contingency operations for the information sys	stem; contingency plan; capacity planning c	locuments; other relevant documents or
records.(Optional)			
	ngency planning and plan implementation responsibilities.(Opti	onal)	
CP-3 – Contingency Training (Moderat	e)		
Control			
	nanagers and users of the information system) shall receive tra ystem. Refresher training shall be provided to all contingency		tand their contingency roles and
Guidance			
Managers, responsible for contingency operation	ons, and technical personnel should meet, at a minimum, once training has been completed	a year for review of contingency policies an	nd procedures. Each review session should

be documented and confirmed that appropriate training has been completed.

Applicability: All	References: ARS: CP-3; FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3	Related Controls:
ASSESSMENT PROCEDURE: CP-3.1		
Assessment Objective		
Determine if:		
	g to personnel with significant contingency roles and responsibilities;	
(ii) the organization records the type of continge		
(iii) the organization defines frequency of refres	ner contingency training; and	
(iv) the organization provides initial training and	refresher training in accordance with organization-defined frequency, at least annually.	
Assessment Methods And Objects		
plan; other relevant documents or records.	ency plan; procedures addressing contingency training; contingency training curriculum; contingency train	ning material; information system security
Interview: Organizational personnel with contin	gency planning, plan implementation, and training responsibilities.	
ASSESSMENT PROCEDURE: CP-3.2		
Assessment Objective		
Determine if contingency training material addre	esses the procedures and activities necessary to fulfill identified organizational contingency roles and resp	oonsibilities.
Assessment Methods And Objects		
Examine: Contingency planning policy; conting records.	ency plan; procedures addressing contingency training; contingency training curriculum; contingency train	ning material; other relevant documents or
CP-3(0) – Enhancement (Moderate)		
Control		
Provide training every 365 days in contingency	roles and responsibilities.	
Applicability: All	References: ARS: CP-3(0); FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP:	Related Controls:
	4.6.3	
ASSESSMENT PROCEDURE: CP-3(0).1		
Assessment Objective		
Determine if the organization meets the require Assessment Methods And Objects	ments as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ying enhancement to the baseline control.
-	ency plan; procedures addressing contingency training; contingency training curriculum; contingency trair	ning material information system security pla
(for organization-defined frequency for refreshe	contingency training); other relevant documents or records. gency planning, plan implementation, and training responsibilities.	
CP-4 – Contingency Plan Testing and E		
Control		
	ery 365 days using defined tests and exercises, such as the tabletop test in accordance with current CMS	S Procedures to determine the plans'
	. Test / exercise results shall be documented and reviewed by appropriate organization officials. Reason	
be initiated to close or reduce the impact of CP		
Guidance		
	ercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, func	tional/tabletop exercises). The depth and
rigor of contingency plan testing and/or exercise	is increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or ex	ercises also include a determination of the
	(e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance	
	hs for information technology plans and capabilities.	, , , , , , , , , , , , , , , , , , , ,
Applicability: All	References: ARS: CP-4; FISCAM: TSC-1.1, TSC-4.1, TSC-4.2.1, TSC-4.2.2; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2; NIST 800-53/53A:	Related Controls:
	CP-4; PISP: 4.6.4	
ASSESSMENT PROCEDURE: CP-4.1		
Assessment Objective		
Determine if:		
(i) the organization defines the frequency of con	tingency plan tests and/or exercises;	

(ii) the organization defines the set of conting	ency plan tests and/or exercises.	
	ngency plan using organization-defined tests/exercises in accordance with organization-defined frequency;	
(iv) the organization documents the results of		
	blan test/exercise results and takes corrective actions.	
Assessment Methods And Objects		
•	ngency plan, procedures addressing contingency plan testing and exercises; information system security pl records.	lan; contingency plan testing and/or exercise
ASSESSMENT PROCEDURE: CP-4.2		
Assessment Objective		
Determine if the contingency plan tests/exercit	ises address key aspects of the plan	
Assessment Methods And Objects		
•	ngency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/	or exercise documentation; contingency plan
CP-4(0) – Enhancement (Moderate)		
Control		
	ed using a combination of tabletop exercises and operational tests every 365 days, and updated as needed	4
Applicability: All	References: ARS: CP-4(0); FISCAM: TSC-4.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-4; PISP:	Related Controls:
	4.6.4	Related Controls.
ASSESSMENT PROCEDURE: CP-4(0).1		
Assessment Objective		
-	rements as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ving enhancement to the baseline control.
Assessment Methods And Objects		
•	ngency plan, procedures addressing contingency plan testing and exercises; information system security pl	an (for the organization-defined frequency of
	he list of the organization-defined contingency plan tests and/or exercises); contingency plan testing and/o	
documents or records.		· · · · · · · · · · · · · · · · · · ·
CP-4(1) – Enhancement (Moderate)		
Control		
Coordinate testing and exercising of CP with	parties responsible for related plans, such as:	
(a) Business Continuity Plan,		
(b) Disaster Recovery Plan,		
(c) Continuity of Operations Plan,		
(d) Business Recovery Plan, and		
(e) Incident Response Plan.		
Guidance		
Examples of related plans include Business C	Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident F	
Applicability: All	References: ARS: CP-4(1); HSPD 7: G(22)(i); NIST 800-53/53A: CP-4(1)	Related Controls:
ASSESSMENT PROCEDURE: CP-4(1).1		
Assessment Objective		
	ntingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Bus s Recovery Plan, Incident Response Plan, Emergency Action Plan).	iness Continuity Plan, Disaster Recovery
Assessment Methods And Objects		
	ngency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/	or exercise documentation; other relevant
	tingency planning, plan implementation, and testing responsibilities.	
CP-5 – Contingency Plan Update (Mo		
Control		
CPs shall be reviewed at least every 365 days	s and, if necessary, revised to address system / organizational changes and/or any problems encountered	during plan implementation, execution, or
Rev. 9	Page 66 of 189	BPSSM Appendix A, Attachment

testing.		
Guidance		
	ges in mission, functions, or business processes supported by the information system. The organization commun s (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Pla	
Applicability: All	References: ARS: CP-5; FISCAM: TSC-1.1, TSC-3.1.5; HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	Related Controls:
ASSESSMENT PROCEDURE: CP-5	1	
Assessment Objective Determine if: (i) the organization defines the freque (ii) the organization updates the cont (iii) the revised plan addresses the sy Assessment Methods And Objects Examine: Contingency planning poli ASSESSMENT PROCEDURE: CP-5 Assessment Objective Determine if the organization communication Assessment Methods And Objects Examine: Contingency planning poli Interview: Organizational personnel CP-5(0) – Enhancement (Moderate) Control Review the CP at least every 365 da	ency of contingency plan reviews and updates; ngency plan in accordance with organization-defined frequency, at least annually; and rstem/organizational changes identified by the organization or any problems encountered by the organization dur cy; contingency plan; procedures addressing contingency plan reviews and updates; information system security 2 nicates necessary changes to the contingency plan to other organizational elements with related plans. cy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents o with contingency plan update responsibilities; organizational personnel with mission-related and operational resp ys and update, as necessary, to address: system, organizational, or facility changes; problems encountered durin	plan; other relevant documents or records.
other conditions that may impact the pplicability: All	system CP. References: ARS: CP-5(0); HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	Related Controls:
ASSESSMENT PROCEDURE: CP-5		
Assessment Objective		
-	he requirements as specified in the baseline control and the specific CMS requirements as prescribed in this am	olifying enhancement to the baseline control.
Assessment Methods And Objects		
	cy; contingency plan; procedures addressing contingency plan reviews and updates; information system security s); other relevant documents or records.	plan (for organization-defined frequency of
	cy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents o	
	with contingency plan review and update responsibilities; organizational personnel with mission-related and oper	ational responsibilities.
CP-6 – Alternate Storage Site (Moderate)	
Control		
stored in a secure location at an alter	e site shall be established and implemented effectively to permit the storage of CMS information system backup i nate site accessible by management and other key personnel. Procedures shall be developed, documented, and of routine information system operations and the alternate storage site.	
Suidance		
	backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent	t with the organization's recovery time objective
Applicability: All	References: ARS: CP-6; IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6; PISP: 4.6.6	Related Controls:
ASSESSMENT PROCEDURE: CP-6		•
Assessment Objective		
Determine if:		
(i) the organization identifies an alter	nate storage site; and	
Pau 0	Dage 67 of 190	DDSSM Annondix A Attachmon

(ii) alternate storage site agreements are	currently in place (if needed) to permit stor	age of information system backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-6.2

Assessment Objective

Determine if the alternate storage site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information consistent with the organization's recovery time objectives and recovery point objectives.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

Interview: Organizational personnel with alternate storage site responsibilities.(Optional)

CP-6(1) – Enhancement (Moderate)

Control

Ensure that the alternate storage site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.

 Applicability: All
 References: ARS: CP-6(1); FISCAM: TSC-2.1.3; IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(1)
 Related Controls:

ASSESSMENT PROCEDURE: CP-6(1).1

Assessment Objective

Determine if:

(i) the contingency plan identifies the primary storage site hazards; and

(ii) the alternate storage site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.

CP-6(3) – Enhancement (Moderate)

Control

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and document explicit mitigation actions.

Applicability: All	References: ARS: CP-6(3); IRS-1075: 5.6.2.2#1.4; NIST 800-53/53A: CP-6(3)	Related Controls:	
ASSESSMENT PROCEDURE:	CP-6(3).1		
Assessment Objective			
Determine if:			
(i) the contingency plan identified	es potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and		
(ii) the contingency plan define	s explicit mitigation actions for potential accessibility problems.		
Assessment Methods And Ob	jects		
Examine: Contingency plannin	g policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant docume	nts or records.	
CP-7 – Alternate Processin	g Site (Moderate)		
Control			
	processing site shall be established and implemented to permit the resumption of CMS information system operations fo		
	are unavailable, and the CP calls for application recovery in place of other accepted processes. Procedures shall be de	veloped, documented, and implemented	
effectively to establish contingency activities and responsibilities.			
Guidance			
Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives.			
Applicability: All	References: ARS: CP-7; FISCAM: TSC-3.2.1; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7; PISP 4.6.7	Related Controls:	
ASSESSMENT PROCEDURE: CP-7.1			
Assessment Objective			
Determine if:			
(i) the organization identifies an alternate processing site;			

(ii) the organization defines the time period within which processing must be resumed at the alternate processing site; and (iii) alternate processing site agreements are currently in place (if needed) to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-7.2

Assessment Objective

Determine if the alternate processing site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records. **Interview:** Organizational personnel with alternate processing site responsibilities.(Optional)

CP-7(0) – Enhancement (Moderate)

Control

Ensure all equipment and supplies required for resuming information system operations for critical functions within seventy-two (72) hours after COOP activation are available at the alternate processing site, or contracts are in place to support delivery to the site.

Applicability: All	References: ARS: CP-7(0); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7; PISP: 4.6.7	Related Controls:
ASSESSMENT PROCEDURE: CP-7(0).1		

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan (for organization-defined time period within which processing must be resumed at the alternate processing site); other relevant documents or records.

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

Interview: Organizational personnel with alternate processing site responsibilities.(Optional)

CP-7(1) – Enhancement (Moderate)

Control

Ensure the alternate processing site is geographically separated from the primary processing site, to prevent susceptibility to the same hazards.

Applicability: All	References: ARS: CP-7(1); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(1)	Related Controls:

ASSESSMENT PROCEDURE: CP-7(1).1

Assessment Objective

Determine if:

(i) the contingency plan identifies the primary processing site hazards; and

(ii) the alternate processing site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

CP-7(2) – Enhancement (Moderate)

Control

Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Applicability: All	References: ARS: CP-7(2); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(2)	Related Controls:
ASSESSMENT PROCEDURE: CP-7(2).1		

Assessment Objective

Determine if:

(i) the contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and

(ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.

Assessment Methods And Objects				
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.				
CP-7(3) – Enhancement (Moderate)				
Control				
Ensure alternate processing site agreements con				
Applicability: All	References: ARS: CP-7(3); FISCAM: TSC-3.2.1; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-7(3)	Related Controls:		
ASSESSMENT PROCEDURE: CP-7(3).1				
Assessment Objective				
Determine if alternate processing site agreement	ts contain priority-of-service provisions in accordance with the organization's availability requirements.			
Assessment Methods And Objects				
Examine: Contingency planning policy; contingen	ncy plan; procedures addressing alternate processing sites; alternate processing site agreements; other	r relevant documents or records.		
CP-8 – Telecommunications Services (I	Moderate)			
Control				
Necessary agreements shall be established and primary operations and communications capabili	implemented for alternate communications services capable of restoring adequate communications to a ties are unavailable.	accomplish mission critical functions when the		
Guidance				
	ecommunications services are provided by a common carrier, the organization requests Telecommunicat	tions Service Priority (TSP) for all		
	ecurity emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).	,		
Applicability: All	References: ARS: CP-8; FISCAM: TSC-3.2.2; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8; PISP:	Related Controls:		
	4.6.8			
ASSESSMENT PROCEDURE: CP-8.1				
Assessment Objective				
Determine if:				
	te telecommunications services to support the information system;			
	n which resumption of information system operations must take place; and			
	nents are in place to permit the resumption of telecommunications services for critical mission/business f	functions within the organization-defined time		
period when the primary telecommunications cap	babilities are unavailable.			
Assessment Methods And Objects				
	ncy plan; procedures addressing alternate telecommunications services; information system security plan	an; primary and alternate telecommunications		
service agreements; other relevant documents o ASSESSMENT PROCEDURE: CP-8.2				
Assessment Objective				
Determine if:	requiration are used for notional equivity emergency prepared aces and			
	rganization are used for national security emergency preparedness; and			
(ii) a common carrier provides telecommunicatio	is services.			
Assessment Methods And Objects		munications convice corresponder other		
relevant documents or records.	ncy plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications	nunications service agreements, other		
CP-8(0) – Enhancement (Moderate)				
Control				
Resume system operations for critical functions within seventy-two (72) hours when the primary telecommunications capabilities are unavailable.				
Applicability: All References: ARS: CP-8(0); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8; PISP: 4.6.8 Related Controls:				
ASSESSMENT PROCEDURE: CP-8(0).1				
Assessment Objective	ponto an apposition in the baseline control and the appositio CMC requirements on preserviced in this appolit	ving onhoncomont to the baseling control		
Determine if the organization meets the requirem	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ying emiancement to the baseline control.		

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; information system security plan (for organization-defined time period within which resumption of information system operations must take place); primary and alternate telecommunications service agreements; other relevant documents or records. Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.

CP-8(1) – Enhancement (Moderate)

Control

Ensure agreements with pr	nary and alternate telecommunication service providers include priority-of-service provisions.	
Applicability: All	References: ARS: CP-8(1); FISCAM: TSC-3.2.2; IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(1)	Related Controls:
ASSESSMENT PROCEDUR	E: CP-8(1).1	
Assessment Objective		
Determine if primary and a contingency plan.	ernate telecommunications service agreements contain priority-of-service provisions in accordance with the availability requir	rements defined in the organization's
Assessment Methods And	Dbjects	
Examine: Contingency pla relevant documents or reco	ning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecomr ds.	nunications service agreements; other
CP-8(2) – Enhancement (M	derate)	
Control		
Ensure alternate telecomm	inication providers do not share a single point of failure with primary telecommunications services.	
Applicability: All	References: ARS: CP-8(2); IRS-1075: 5.6.2.2#1.5; NIST 800-53/53A: CP-8(2)	Related Controls:
ASSESSMENT PROCEDUR	E: CP-8(2).1	
Assessment Objective		
Determine if primary and a	ernate telecommunications services share a single point of failure.	
Assessment Methods And	Objects	
	ning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecomr	nunications service agreements; other
relevant documents or reco		
	ersonnel with contingency planning and plan implementation responsibilities; telecommunications service providers.	
CP-9 – Information Syst	m Backup (Moderate)	
Control		
(including system state info	e in place and supporting procedures shall be developed, documented, and implemented effectively to enable the backing-up mation) contained in the CMS information system. The frequency of information system backups and the transfer rate of backing-up sistent with the CMS recovery time objectives and recovery point objectives.	
	or sufficient backup storage capability. Checkpoint capabilities shall be part of any backup operation that updates files and co	

time. Backup copies of CMS data shall be created on a regular basis, and appropriate safeguards shall be implemented to protect the technical and physical security of backup media at the storage location. Where appropriate, backup copies of all other forms of data, including paper records, shall be created based upon an assessment of the level of data criticality and the corresponding risk of data loss.

Guidance

The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. Checkpoint and restart capabilities are part of any operation that updates files and consumes large amounts of computer time. The protection of system backup information while in transit is beyond the scope of this control.

Applicability: All	References: ARS: CP-9; FISCAM: TSC-2.1.1, TSC-2.1.3; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1);	Related Controls: MA-CMS-1, MA-CMS-2,
	IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9.1

Assessment Objective

Determine if:

(i) the organization defines the frequency of information systems backups:

(ii) the organization defines the user-level and system-level information (including system state information) that is required to be backed up; and

(iii) the organization identifies the location(s) for storing backup information.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records.

ASSESSMENT PROCEDURE: CP-9.2

Assessment Objective

Determine if:

(i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency;

(ii) the organization stores backup information in designated locations in accordance with information system backup procedures; and

(iii) the organization protects backup information at the designated storage locations.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records.

CP-9(0) – Enhancement (Moderate)

Control

Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time and action.

Applicability: All	References: ARS: CP-9(0); HIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A:	Related Controls:
	CP-9; PISP: 4.6.9	

ASSESSMENT PROCEDURE: CP-9(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects**

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for information system backup); backup storage location(s); other relevant documents or records.

CP-9(1) – Enhancement (Moderate)

Control

Test backup information to verify media reliability and information integrity, following each backup.

Applicability: All	References: ARS: CP-9(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(1)	Related Controls:

ASSESSMENT PROCEDURE: CP-9(1).1

Assessment Objective

Determine if:

(i) the organization defines the frequency of information system backup testing:

(ii) the organization conducts information system backup testing within the organization-defined frequency; and

(iii) testing results verify backup media reliability and information integrity.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; information system backup test results; backup storage location(s); other relevant documents or records.

CP-9(4) – Enhancement (Moderate)

Control

Protect backup information from unauthorized modification.

The organization employs appropriate mechan		
	isms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups.	Protecting the confidentiality of system
backup information is beyond the scope of this		
Applicability: All	References: ARS: CP-9(4); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9(4)	Related Controls: MP-4, MP-5
ASSESSMENT PROCEDURE: CP-9(4).1		
Assessment Objective		
	ate mechanisms to protect the integrity of information system backup information.	
Assessment Methods And Objects		
	gency plan; procedures addressing information system backup; information system design documentation;	backup storage location(s); information
	ocumentation; other relevant documents or records.	
Interview: Organizational personnel with inforr	nation system backup responsibilities.	
CP-9(PII-1) – Enhancement (Moderate)		
Control		
Insure that a current, retrievable, copy of PII is	available before movement of servers.	
Applicability: All	References: HIPAA: 164.310(d)(2)(iv)	Related Controls:
ASSESSMENT PROCEDURE: CP-9(PII-1).1		·
Assessment Objective		
-	t and retrievable copy of PII is available before movement of servers.	
Assessment Methods And Objects		
	esses in the COOP and backup procedures are available. A current copy of PII is available.	
	ackup responsibilities to determine if the PII copy is current and retrievable.	
	ition procedures for PII, determine if the current copy is retrievable.	
CP-10 – Information System Recovery		
Control		
	mechanisms with supporting procedures shall be developed, documented, and implemented effectively to	allow the CMS information system to be
	state after a disruption or failure. Recovery of CMS information systems after a failure or other contingen	
verifiable manner.		
Guidance		
Information system recovery and reconstitutior	to a known secure state means that all system parameters (either default or organization-established) are	e set to secure values, security-critical patche
	ettings are reestablished, system documentation and operating procedures are available, application and s	system software is reinstalled and configured
	recent, known secure backups is loaded, and the system is fully tested.	
		1
Applicability: All	References: ARS: CP-10; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10;	Related Controls:
	References: ARS: CP-10; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10; PISP: 4.6.10	Related Controls:
ASSESSMENT PROCEDURE: CP-10.1		Related Controls:
		Related Controls:
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective	PISP: 4.6.10	
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea	PISP: 4.6.10	
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects	PISP: 4.6.10	hes, configuration settings, and
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects Examine: Contingency planning policy; conting	PISP: 4.6.10	hes, configuration settings, and
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects Examine: Contingency planning policy; conting	PISP: 4.6.10	hes, configuration settings, and
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects Examine: Contingency planning policy; conting documentation; information system design doc	PISP: 4.6.10	hes, configuration settings, and
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects Examine: Contingency planning policy; conting documentation; information system design doc ASSESSMENT PROCEDURE: CP-10.2 Assessment Objective	PISP: 4.6.10	hes, configuration settings, and nfiguration settings and associated
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects Examine: Contingency planning policy; conting documentation; information system design doc ASSESSMENT PROCEDURE: CP-10.2 Assessment Objective	PISP: 4.6.10 ans for capturing the information system's operational state including appropriate system parameters, pato ruption or failure. gency plan; procedures addressing information system recovery and reconstitution; information system co umentation; other relevant documents or records.	hes, configuration settings, and nfiguration settings and associated
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects Examine: Contingency planning policy; conting documentation; information system design doc ASSESSMENT PROCEDURE: CP-10.2 Assessment Objective Determine if the organization makes available Assessment Methods And Objects Examine: Contingency planning policy; conting	PISP: 4.6.10 ans for capturing the information system's operational state including appropriate system parameters, pater ruption or failure. gency plan; procedures addressing information system recovery and reconstitution; information system co- umentation; other relevant documents or records.	hes, configuration settings, and nfiguration settings and associated wn secure state after disruption or failure.
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects Examine: Contingency planning policy; conting documentation; information system design doc ASSESSMENT PROCEDURE: CP-10.2 Assessment Objective Determine if the organization makes available Assessment Methods And Objects Examine: Contingency planning policy; conting documentation; information system design doc	PISP: 4.6.10 ans for capturing the information system's operational state including appropriate system parameters, pater ruption or failure. gency plan; procedures addressing information system recovery and reconstitution; information system co- umentation; other relevant documents or records. and applies mechanisms and procedures for recovery and reconstitution of the information system to know gency plan; procedures addressing information system recovery and reconstitution; information system to know gency plan; procedures addressing information system recovery and reconstitution; information system to know gency plan; procedures addressing information system recovery and reconstitution; information system co- umentation; other relevant documents or records.	hes, configuration settings, and nfiguration settings and associated wn secure state after disruption or failure.
ASSESSMENT PROCEDURE: CP-10.1 Assessment Objective Determine if the organization identifies the mea application/system software prior to system dis Assessment Methods And Objects Examine: Contingency planning policy; conting documentation; information system design doc ASSESSMENT PROCEDURE: CP-10.2 Assessment Objective Determine if the organization makes available Assessment Methods And Objects Examine: Contingency planning policy; conting documentation; information system design doc	PISP: 4.6.10 ans for capturing the information system's operational state including appropriate system parameters, pater ruption or failure. gency plan; procedures addressing information system recovery and reconstitution; information system co- umentation; other relevant documents or records.	hes, configuration settings, and nfiguration settings and associated wn secure state after disruption or failure.

CP-10(0) – Enhancement (Me	iderate)	
Control		
Secure information system re	covery and reconstitution includes, but not limited to:	
(a) Reset all system paramet	ers (either default or organization-established),	
(b) Reinstall patches,		
(c) Reestablish configuration	settings,	
(d) Reinstall application and	ystem software, and	
(e) Fully test the system.		
Applicability: All	References: ARS: CP-10(0); NIST 800-53/53A: CP-10; PISP: 4.6.10	Related Controls:
ASSESSMENT PROCEDURE	: CP-10(0).1	
ssessment Objective		
Determine if the organization	meets the requirements as specified in the baseline control and the specific CMS requirements as prescrib	ed in this amplifying enhancement to the baseline control.
Assessment Methods And C	bjects	
Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Test: Automated mechanisms implementing information system recovery and reconstitution operations.

Identification and Authentication (IA) – Technical

IA-1 – Identification and Authentication Policy and Procedures (Moderate)

Control

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

Guidance

The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and SP 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	References: ARS: IA-1; IRS-1075: 5.6.3.1#1.1; NIST 800-53/53A: IA-1; PISP: 4.7.1	Related Controls:
ASSESSMENT PROCEDURE: IA-1.1		

Assessment Objective

Determine if:

(i) the organization develops and documents identification and authentication policy and procedures;

(ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review identification and authentication policy and procedures; and

(iv) the organization updates identification and authentication policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.

Interview: Organizational personnel with identification and authentication responsibilities.(Optional)

ASSESSMENT PROCEDURE: IA-1.2

Assessment Objective

Determine if:

(i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.

Interview: Organizational personnel with identification and authentication responsibilities.(Optional)

IA-2 – User Identification and Authentication (Moderate)

Control

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique IA of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

Guidance

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in SP 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST SP 800-63 level 1 compliant. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide information security for the organization.

In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST SP 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals. References: ARS: IA-2; FISCAM: TAC-3.2.A.4, TAN-2.1.4; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-Related Controls: AC-14, AC-17, MA-4 Applicability: All 1075: 5.6.3.1#1.2. 5.6.3.3#2.3: NIST 800-53/53A: IA-2: PISP: 4.7.2 **ASSESSMENT PROCEDURE: IA-2.1** Assessment Objective Determine if: (i) the information system uniquely identifies and authenticates users (or processes acting on behalf of users); and (ii) authentication levels for users (or processes acting on behalf of users) are consistent NIST SP 800-63 and e-authentication risk assessment results. Assessment Methods And Objects Examine: Identification and authentication policy: NIST SP 800-63: procedures addressing user identification and authentication: information system design documentation: e-authentication risk assessment results; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Test: Automated mechanisms implementing identification and authentication capability for the information system. IA-2(1) – Enhancement (Moderate) Control Employ multifactor authentication for remote system access that is at least NIST SP 800-63 level 3 compliant. Applicability: All References: ARS: IA-2(1); FISCAM: TAN-2.1.7; HIPAA: 164.312(d); IRS-1075: 5.6.3.1#1.2; NIST **Related Controls:** 800-53/53A: IA-2(1) ASSESSMENT PROCEDURE: IA-2(1).1 Assessment Objective Determine if: (i) the organization defines the NIST SP 800-63 authentication levels for the information system; and (ii) the information system employs multifactor authentication for remote system access that is NIST SP 800-63 compliant in accordance with the organizational selection of level 3, level 3 using a hardware authentication device, or level 4. **Assessment Methods And Objects** Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. IA-2(CMS-1) – Enhancement (Moderate) Control Require the use of unique user identifiers and system and/or network authenticators. References: ARS: IA-2(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4, TAN-2.1.4, TAN-2.1.7; IRS-Applicability: All **Related Controls:** 1075: 5.6.3.1#1.2

ASSESSMENT PROCEDURE: IA-2(CMS-1).1

Assessment Objective

Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine the use of unique user identifiers and system and/or network authenticators is required.

Interview: Organizational personnel with identification and authentication responsibilities to determine the use of unique user identifiers and system and/or network authenticators is required. Test: Automated mechanisms implementing identification and authentication capability for the information system to determine the use of unique user identifiers and system and/or network authenticators is required.

IA-2(CMS-2) – Enhancement (Moderate)

Control

All passwords shall be encrypted in transit and at rest.

Applicability: All	References: ARS: IA-2(CMS-2); FISCAM: TAC-3.2.A.1, TAC-3.2.A.7; IRS-1075: 5.6.3.1#1.2	Related Controls:
SSESSMENT PROCEDURE: IA-2(CM	IS-2).1	
ssessment Objective		
Determine if authentication levels for use	ers (or processes acting on behalf of users) are consistent NIST SP 800-63.	
ssessment Methods And Objects		
Examine: Identification and authenticati	on policy; NIST SP 800-63; procedures addressing user identification and authentication; information system	n design documentation; information system
configuration settings and associated do	ocumentation; information system audit records; other relevant documents or records to determine all passwo	ords are required to be encrypted in transit and
rest.		
o 1	h identification and authentication responsibilities to determine to determine all passwords are required to be	51
	nting identification and authentication capability for the information system to determine all passwords are rec	quired to be encrypted in transit and at rest.
A-2(CMS-3) – Enhancement (Moderat	e)	
Control		
Help desk support requires user identific	ation for any transaction that has information security implications.	
pplicability: All	References: ARS: IA-2(CMS-3)	Related Controls:
SSESSMENT PROCEDURE: IA-2(CM	IS-3).1	
ssessment Objective		
	ers (or processes acting on behalf of users) are consistent NIST SP 800-63.	
ssessment Methods And Objects		
	on policy; NIST SP 800-63; procedures addressing user identification and authentication; information system	design documentation: information system
	cumentation; information system audit records; other relevant documents or records to determine help desk	
transaction that has information security		
Interview: Organizational personnel with	h identification and authentication responsibilities to determine to determine help desk support requires user	identification for any transaction that has
information security implications.		
	nting identification and authentication capability for the information system to determine help desk support re	quires user identification for any transaction the
has information security implications.		
A-3 – Device Identification and A	thentication (Moderate)	
Control		
Automated mechanisms shall be used to	p enable IA of the CMS information system being used and to which a connection is being made before estal	blishing a connection.
Buidance		
The information system typically uses eit	ther shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet	Protocol (TCP/IP) addresses) or an
organizational authentication solution (e.	g., IEEE 802. 1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Laye	r Security (TLS) authentication) to identify and
	e area networks. The required strength of the device authentication mechanism is determined by the FIPS 1	99 security categorization of the information
system with higher impact levels requirir		
pplicability: All	References: ARS: IA-3; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	Related Controls:
SSESSMENT PROCEDURE: IA-3.1		
ssessment Objective		
Determine if:		
	ces requiring identification and authentication before establishing connections to the information system; and	
(ii) the information system identifies and	authenticates specific devices identified by the organization before establishing connections.	
ssessment Methods And Objects		
Examine: Identification and authenticati	on policy; procedures addressing device identification and authentication; information system design docume	entation; device connection reports; informatior
	iated documentation; other relevant documents or records.	
	nting device identification and authentication.(Optional)	
A-3(0) – Enhancement (Moderate)		
Control		
	ses either a shared secret or digital certificate to identify and authenticate specific devices before establishing	g a connection.
	ses either a shared secret or digital certificate to identify and authenticate specific devices before establishing References: ARS: IA-3(0); IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	g a connection. Related Controls:

ASSESSMENT PROCEDURE: IA-3(0).1 **Assessment Objective** Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** Examine: Identification and authentication policy; information system design documentation; procedures addressing device identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing device identification and authentication.(Optional) IA-4 – Identifier Management (Moderate) Control Procedures shall be developed, documented, and implemented effectively to manage user identifiers. The procedures shall address processes and controls for: 4.7.4.1. Identifying each user uniquely; 4.7.4.2. Verifying the identity of each user; 4.7.4.3. Receiving authorization to issue a user identifier from an appropriate organization official; 4.7.4.4. Ensuring that the user identifier is issued to the intended party; 4.7.4.5. Disabling user identifier after a specific period of inactivity: and 4.7.4.6. Archiving user identifiers. Reviews and validation of system users' accounts shall be conducted to ensure the continued need for access to a system. Identifier management shall not be applicable to shared information system accounts (i.e., quest and anonymous) Guidance Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. References: ARS: IA-4; FISCAM: TAC-3.2.A.4, TAN-2.1.4; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: Applicability: All **Related Controls:** IA-4; PISP: 4.7.4 **ASSESSMENT PROCEDURE: IA-4.1 Assessment Objective** Determine if: (i) the organization manages user identifiers by uniquely identifying each user; (ii) the organization manages user identifiers by verifying the identity of each user; (iii) the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official: (iv) the organization manages user identifiers by issuing the identifier to the intended party; (v) the organization defines the time period of inactivity after which a user identifier is to be disabled: (vi) the organization manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and (vii) the organization manages user identifiers by archiving identifiers. **Assessment Methods And Objects** Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. Test: Identity verification capability for the information system and for organizational facilities. **ASSESSMENT PROCEDURE: IA-4.2 Assessment Objective** Determine if the organization uses a Personal Identity Verification (PIV) card token to uniquely identify and authenticate federal employees and contractors in accordance with FIPS 201 and NIST SP 800-73, 800-76, and 800-78,

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST SP 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. Test: Identity verification capability for the information system and for organizational facilities.

IA-4(0) – Enhancement (Moderate)					
Control	wand delete disabled assounts during annual re-partification process				
	y and delete disabled accounts during annual re-certification process. References: ARS: IA-4(0); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.1#2, 5.6.3.2#2.1; NIST 800-	Deleted Controlog AC 2(2)			
Applicability: All	53/53A: IA-4; PISP: 4.7.4	Related Controls: AC-2(3)			
ASSESSMENT PROCEDURE: IA-4(0).1					
Assessment Objective					
Determine if the organization meets the requirem	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ving enhancement to the baseline control.			
Assessment Methods And Objects		5			
	r; procedures addressing identifier management; information system security plan (for organization-defin	ed time period of inactivity after which user			
	esign documentation; information system configuration settings and associated documentation; list of inf				
Test: Identity verification capability for the inform	ation system and for organizational facilities.				
Examine: Identification and authentication policy	r; procedures addressing identifier management; information system design documentation; FIPS 201; N	IST SP 800-73, 800-76, 800-78; information			
	cumentation; list of information system accounts; other relevant documents or records.				
IA-4(CMS-1) – Enhancement (Moderate)					
Control					
Require system administrator to maintain separa	te user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for sys	tem administration activities.			
Applicability: All	References: ARS: IA-4(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4; IRS-1075: 5.6.3.1#2	Related Controls: AC-2(CMS-2)			
ASSESSMENT PROCEDURE: IA-4(CMS-1).1					
Assessment Objective					
Determine if the organization manages user ider	tifiers by uniquely identifying each user.				
Assessment Methods And Objects					
Examine: Identification and authentication policy identifier is to be disabled); information system d	Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration				
activities.	cation and authentication responsibilities to determine system administrators maintain separate user acc	ounts one evolusively for standard user			
functions (e.g., Internet, email, etc.), and one for					
Test: Identity verification capability for the inform functions (e.g., Internet, email, etc.), and one for	ation system and for organizational facilities to determine system administrators maintain separate user system administration activities.	accounts; one exclusively for standard user			
IA-4(CMS-2) – Enhancement (Moderate)					
Control					
	ceive prior written approval from the CIO or his/her designated representative.				
Applicability: All	References: ARS: IA-4(CMS-2)	Related Controls:			
ASSESSMENT PROCEDURE: IA-4(CMS-2).1					
Assessment Objective					
•	ization periodically review identification and authentication policy and procedures.				
Assessment Methods And Objects					
-	 and procedures; other relevant documents or records to determine non-CMS entities receive prior writte entifiers. 	en approval from the CIO or his/her			
Interview: Organizational personnel with identification and authentication management responsibilities to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers.					
IA-4(FIS-1) – Enhancement (Moderate)					
Control					
	sers to remove terminated or transferred employees from the system.				
Applicability: All	References: FISCAM: TAC-3.2.A.6	Related Controls:			
	D 3 0, 0400				

ASSESSMENT PROCEDURE: IA-4(FIS-1).1

Assessment Objective

Determine if the organizational personnel files are automatically [or manually] matched with actual system users to remove terminated or transferred employees from the system.

Assessment Methods And Objects

Examine: Documentation of such comparisons.

Examine: Pertinent policies and procedures.

Interview: Security managers.

IA-5 – Authenticator Management (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to manage user authenticators. The procedures shall address processes and controls for: initial authenticator content; distribution for new, lost, compromised, or damaged authenticators; revocation of authenticators; changing default authenticators; and changing / refreshing authenticators at specified intervals. Users shall not loan or share authenticators with other users. Lost or compromised authenticators shall be reported immediately to appropriate authority.

Selection of passwords or other authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS System Security Level of the information system. Automated mechanisms shall be in place for password-based authentication, to ensure that the information system:

4.7.5.1. Protects passwords from unauthorized disclosure and modification when stored and transmitted;

4.7.5.2. Prohibits passwords from being displayed when entered;

4.7.5.3. Enforces automatic expiration of passwords;

4.7.5.4. Prohibits password reuse for a specified number of generations; and

4.7.5.5. Enforces periodic password changes.

Guidance

Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification authentication.

	IA-5; PISP: 4.7.5	1(CMS-2)
Applicability: All	References: ARS: IA-5; FISCAM: TAC-3.2.A.1, TAC-3.2.A.3; IRS-1075: 5.6.3.1#2; NIST 800-53/53A:	Related Controls: AC-11(0), AC-CMS-

ASSESSMENT PROCEDURE: IA-5.1

Assessment Objective

Determine if:

(i) the organization manages information system authenticators by defining initial authenticator content;

(ii) the organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;

(iii) the organization manages information system authenticators by changing default authenticators upon information system installation; and

(iv) the organization manages information system authenticators by changing/refreshing authenticators periodically.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

Test: Automated mechanisms implementing authenticator management functions.

IA-5(0) – Enhancement (Moderate)

Control

For password-based authentication:

(a) Protect passwords from disclosure or modification when stored or transmitted,

(b) Prevent passwords from being displayed when entered,

(c) When using passwords in connection with e-authentication, refer to ARS Appendix A, e-Authentication Standards for further guidance,

(e) Automatically force users (inclu	rd comprising a minimum of eight (8) alphanumeric and/or special ding administrators) to change account and system account passy		
(f) Automatically force users to sel	ect six (6) unique passwords prior to reusing a previous one, and		
	ictions within a minimum of one (1) day and maximum of sixty (60)	days.	
Applicability: All	References: ARS: IA-5(0); HIPAA: 164.308(a)(5)(ii PISP: 4.7.5)(D); IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5;	Related Controls:
SSESSMENT PROCEDURE: IA	5(0).1		
ssessment Objective			
Determine if the organization mee	s the requirements as specified in the baseline control and the spe	cific CMS requirements as prescribed in this amplify	ving enhancement to the baseline control.
ssessment Methods And Object	ts		
	ntication policy; procedures addressing authenticator management nformation system accounts; other relevant documents or records.		tion system configuration settings and
	lementing authenticator management functions.		
A-5(FIS-1) – Enhancement (Mod	erate)		
Control			
	cards, users: (1) maintain possession of their individual tokens, ca	rds, etc., and (2) understand that they must not loan	or share these with others, and must repo
Applicability: All	References: FISCAM: TAC-3.2.A.8		Related Controls:
ASSESSMENT PROCEDURE: IA			
Assessment Objective			
Determine if:			
	n possession of their individual devices such as tokens or key card	ds. etc.: and	
	tand they must not loan or share their individual tokens, cards, etc		
Assessment Methods And Object		,,,,, ,	
Examine: Pertinent policies and p			
Examine: Token or key card ackr			
Interview: Token and/or key card			
A-5(DIR-1) – Enhancement (Moc			
Control			
For password-based authenticatic	a passwords are:		
(a) unique for specific individuals,			
(b) controlled by the assigned use			
(c) not displayed when entered;			
(d) changed every 60 days, when	an individual changes positions, or when security is breached;		
(e) at least 8 characters in length;			
	er, one upper and lower case character, and one special character	;	
(g) prohibited from reuse for at lea			
	more than once in a 24-hour period; and	and a factor of the factor	
(i) all passwords are encrypted in pplicability: All	ransit and at rest. The use of dictionary names or words as passwork References: FISCAM: TAC-3.2.A.1. TAC-3.2.A.2.		Related Controls:
		TAN-2.1.4	Related Controls.
Assessment Objective	tively uses personal and user identification on one teal for accurit	v in denth	
0	tively uses password and user identification as one tool for security	у ш-аерш.	
Assessment Methods And Object		end in months the CMC measured controls	
	tification policy and acceptable user training policy for completene		
	by the organization's policy for password and user system identific	auon.	
(a) unique for specific individuals,	guide or script check the system password configuration: not groups;		

(b) controlled by the assigned user and not subject to disclosure;	
(c) not displayed when entered; (d) changed every 60 days, when an individual changes positions, or when security is breached;	
(d) changed every 60 days, when an individual changes positions, or when security is breached, (e) at least 8 characters in length:	
(f) must include at least one number, one upper and lower case character, and one special character;	
(g) prohibited from reuse for at least 6 generations;	
(h) prohibited from being changed more than once in a 24-hour period; and	
(i) all passwords are encrypted in transit and at rest. The use of dictionary names or words as passwords is prohibited.	
IA-6 – Authenticator Feedback (Moderate)	
Control	- to the second during the puthentipotion process
Automated mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to obscure feedb to protect the information from possible exploitation / use by unauthorized individuals.	ack to users during the authentication process
Guidance	
The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechan	hism Displaving asterisks when a user types
in a password is an example of obscuring feedback of authentication information.	
Applicability: All References: ARS: IA-6; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-6; PISP: 4.7.6	Related Controls:
ASSESSMENT PROCEDURE: IA-6.1	
Assessment Objective	
Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from po	ssible exploitation/use by unauthorized
individuals.	
Assessment Methods And Objects	
Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records.	system configuration settings and associated
Test: Automated mechanisms implementing authenticator feedback.	
IA-6(0) – Enhancement (Moderate)	
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks).	Related Controls:
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks).	Related Controls:
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6	Related Controls:
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1	
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects	ving enhancement to the baseline control.
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records.	ving enhancement to the baseline control.
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback.	ving enhancement to the baseline control.
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback. IA-7 - Cryptographic Module Authentication (Moderate)	ving enhancement to the baseline control.
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify. Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback. IA-7 – Cryptographic Module Authentication (Moderate) Control Control	ving enhancement to the baseline control. system configuration settings and associated
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback. IA-7 - Cryptographic Module Authentication (Moderate)	ving enhancement to the baseline control. system configuration settings and associated
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback. IA-7 - Cryptographic Module Authentication (Moderate) Control Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of app policies, regulations, standards, and guidance for authentication to a cryptographic module. Guidance	ving enhancement to the baseline control. system configuration settings and associated licable laws, Executive Orders, directives,
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback. IA-7 - Cryptographic Module Authentication (Moderate) Control Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of app policies, regulations, standards, and guidance for authentication to a cryptographic module.	ving enhancement to the baseline control. system configuration settings and associated licable laws, Executive Orders, directives,
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback. IA-7 - Cryptographic Module Authentication (Moderate) Control Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of app policies, regulations, standards, and guidance for authentication to a cryptographic module. Guidance The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptic (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a v Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval. Applicability: All References: ARS: IA-7; NIST 800-53/53A: IA-7; PISP: 4.7.7	ving enhancement to the baseline control. system configuration settings and associated licable laws, Executive Orders, directives,
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback. IA-7 - Cryptographic Module Authentication (Moderate) Control Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of app policies, regulations, standards, and guidance for authentication to a cryptographic module. Guidance The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryf (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a v Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.	ving enhancement to the baseline control. system configuration settings and associated licable laws, Executive Orders, directives, btographic Module Validation Program alidation certificate is specifically revoked.
Control Configure the information system to obscure passwords during the authentication process (e.g., display asterisks). Applicability: All References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6 ASSESSMENT PROCEDURE: IA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplify Assessment Methods And Objects Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information documentation; other relevant documents or records. Test: Automated mechanisms implementing authenticator feedback. IA-7 - Cryptographic Module Authentication (Moderate) Control Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of app policies, regulations, standards, and guidance for authentication to a cryptographic module. Guidance The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptic (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a v Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval. Applicability: All References: ARS: IA-7; NIST 800-53/53A: IA-7; PISP: 4.7.7	ving enhancement to the baseline control. system configuration settings and associated licable laws, Executive Orders, directives, otographic Module Validation Program alidation certificate is specifically revoked. Related Controls:

authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).

Assessment Methods And Objects

Examine: Identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing cryptographic module authentication.

Incident Response (IR) - Operational

IR-1 – Incident Response Policy and Procedures (Moderate)

Control

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed, documented, and implemented effectively to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-61 and current CMS Procedures.

Guidance

The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

			_
	53/53A: IR-1; PISP: 4.8.1		
Applicability: All	References: ARS: IR-1; FISCAM: TSP-3.4; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1; NIST 800-	Related Controls:	

ASSESSMENT PROCEDURE: IR-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents incident response policy and procedures;

(ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review incident response policy and procedures; and

(iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.

Interview: Organizational personnel with incident response planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: IR-1.2

Assessment Objective

Determine if:

(i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.

Interview: Organizational personnel with incident response planning and plan implementation responsibilities.(Optional)

IR-2 – Incident Response Training (Moderate)

Control

All personnel shall be trained in their IR roles and responsibilities with respect to a CMS information system. Personnel shall receive periodic refresher training in IR procedures.

Guidance

Procedures and incident response training implementation should:

(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:

(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.

(2) Executives must receive training in information security basics and policy level training in security planning and management.

(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.

(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.

 security management; and management and imp (b) Provide the CMS information systems securit the systems. (c) Provide information systems security refresh (d) Provide training whenever there is a significal 	onnel must receive training in information security basics; management and implementation olementation level training in system/ application life cycle management, risk management, y awareness material/exposure outlined in NIST guidance on IT security awareness and tra- er training for employees as frequently as determined necessary, based on the sensitivity on the change in the information system environment or procedures or when an employee enter	and contingency planning. aining to all new employees before allowing them access to of the information that the employees use or process.
training. Applicability: All	References: ARS: IR-2; IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-2; PISP: 4.8.2	Related Controls:
ASSESSMENT PROCEDURE: IR-2.1	References: ANO: IN 2, INO 1073: 3.0.2.0#2.1 2, NIOT 000 30/00A. IN 2, 1101 : 4.0.2	Inclated Controls.
Assessment Objective		
Determine if: (i) the organization identifies and documents per- (ii) the organization provides incident response tr (iii) incident response training material addresses (iv) the organization defines the frequency of refr (v) the organization provides refresher incident reference Assessment Methods And Objects Examine: Incident response policy; procedures a relevant documents or records.	esponse training in accordance with organization-defined frequency, at least annually. addressing incident response training; incident response training material; information syste	
ě 1	t response training and operational responsibilities.	
IR-2(0) – Enhancement (Moderate)		
Control	apparaibilities of personnel over 265 days	
Provide training on incident response roles and r Applicability: All	References: ARS: IR-2(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-2; PISP: 4.8.2	Related Controls:
ASSESSMENT PROCEDURE: IR-2(0).1	References. ANS. IN-2(0), INS-1075. 3.0.2.0#2.1-2, INST 800-33/35A. IN-2, FISF. 4.6.2	Related Controls.
Assessment Objective		
	nents as specified in the baseline control and the specific CMS requirements as prescribed	in this amplifying enhancement to the baseline control
Assessment Methods And Objects		
Examine: Incident response policy; procedures	addressing incident response training; incident response training material; information systesponse training records; other relevant documents or records.	em security plan (for organization-defined frequency for
	t response training and operational responsibilities.	
IR-3 – Incident Response Testing and Ex	(ercises (Moderate)	
Control		
The IR capability for a CMS information system s results, procedures, and exercises employed to a	shall be tested periodically using appropriate tests, procedures, automated mechanisms, ar conduct the test shall be documented.	d exercises to determine the plan's effectiveness. The test
Guidance		
	ing, and exercise programs for information technology plans and capabilities.	
	References: ARS: IR-3; IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3	Related Controls:
ASSESSMENT PROCEDURE: IR-3.1		
(iv) the organization documents the results of inc Assessment Methods And Objects	lent response tests/exercises; response capability for the information system using organization-defined tests/exercises in	

IR-3(0) – Enhancement (Moderate) Control		
	incident response capability every 365 days, using reviews, analyses, and simulations.	
Applicability: All	References: ARS: IR-3(0); IRS-1075: 5.6.2.6#2.1-2; NIST 800-53/53A: IR-3; PISP: 4.8.3	Related Controls:
ASSESSMENT PROCEDURE: IR-3(0)		
Assessment Objective		
-	e requirements as specified in the baseline control and the specific CMS requirements as prescribed in this a	amplifying enhancement to the baseline control.
Assessment Methods And Objects		
Examine: Incident response policy; pro	ocedures addressing incident response testing and exercises; information system security plan (for list of org tests/exercises); incident response testing material; incident response test results; other relevant documents	panization-defined tests/exercises and organizat
IR-4 – Incident Handling (Modera		
Control		
An incident handling capability, which in	ncludes preparation, identification, containment, eradication, recovery, and follow-up capabilities in response nes, computer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learner	
Guidance		
	ained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical ac	
	ons learned from ongoing incident handling activities into the incident response procedures and implements to	
Applicability: All	References: ARS: IR-4; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800- 53/53A: IR-4; PISP: 4.8.4	Related Controls: AU-6, PE-6, SI-2
ASSESSMENT PROCEDURE: IR-4.1		
Assessment Objective		
Determine if:		
(i) the organization implements an incid	lent handling capability for security incidents that includes preparation, detection and analysis, containment,	eradication, and recovery; and
(ii) the incident handling capability is co		
Assessment Methods And Objects		
Examine: Incident response policy; pro	ocedures addressing incident handling; NIST SP 800-61; other relevant documents or records.	
Interview: Organizational personnel wi		
Test: Incident handling capability for th		
IR-4(1) – Enhancement (Moderate)		
IR-4(1) – Enhancement (Moderate) Control		
Control	e organization.(Optional)	
Control Employ automated mechanisms to sup	e organization.(Optional) port the incident handling process.	Related Controls:
Control Employ automated mechanisms to sup Applicability: All	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1)	Related Controls:
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1)	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1)	Related Controls:
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) .1	Related Controls:
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1)	Related Controls:
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) .1 automated mechanisms to support the incident handling process.	
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro-	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) .1 automated mechanisms to support the incident handling process. becedures addressing incident handling; automated mechanisms supporting incident handling; other relevant of the incident handling is a support of the incide	
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro Interview: Organizational personnel wi	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) .1 automated mechanisms to support the incident handling process. Decedures addressing incident handling; automated mechanisms supporting incident handling; other relevant th incident handling responsibilities.(Optional)	
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro Interview: Organizational personnel wi IR-4(CMS-1) – Enhancement (Modera	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) .1 automated mechanisms to support the incident handling process. Decedures addressing incident handling; automated mechanisms supporting incident handling; other relevant th incident handling responsibilities.(Optional)	
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro Interview: Organizational personnel wi IR-4(CMS-1) – Enhancement (Modera Control	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) .1 automated mechanisms to support the incident handling process. pcedures addressing incident handling; automated mechanisms supporting incident handling; other relevant of th incident handling responsibilities.(Optional) ite)	documents or records.
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro Interview: Organizational personnel wi R-4(CMS-1) – Enhancement (Modera Control Document relevant information related	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) automated mechanisms to support the incident handling process. pocedures addressing incident handling; automated mechanisms supporting incident handling; other relevant of th incident handling responsibilities.(Optional) tte) to a security incident according to CMS Information Security Incident Handling and Breach Notification Process	documents or records.
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro Interview: Organizational personnel wi IR-4(CMS-1) – Enhancement (Modera Control Document relevant information related Applicability: All	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) automated mechanisms to support the incident handling process. becedures addressing incident handling; automated mechanisms supporting incident handling; other relevant of th incident handling responsibilities.(Optional) to a security incident according to CMS Information Security Incident Handling and Breach Notification Proced References: ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	documents or records.
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro Interview: Organizational personnel wi IR-4(CMS-1) – Enhancement (Modera Control Document relevant information related Applicability: All ASSESSMENT PROCEDURE: IR-4(CI	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) automated mechanisms to support the incident handling process. becedures addressing incident handling; automated mechanisms supporting incident handling; other relevant of th incident handling responsibilities.(Optional) to a security incident according to CMS Information Security Incident Handling and Breach Notification Proced References: ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	documents or records. edures.
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro Interview: Organizational personnel wi IR-4(CMS-1) – Enhancement (Modera Control Document relevant information related Applicability: All ASSESSMENT PROCEDURE: IR-4(CI Assessment Objective	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) automated mechanisms to support the incident handling process. becedures addressing incident handling; automated mechanisms supporting incident handling; other relevant of th incident handling responsibilities.(Optional) to a security incident according to CMS Information Security Incident Handling and Breach Notification Proced References: ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	documents or records. edures.
Control Employ automated mechanisms to sup Applicability: All ASSESSMENT PROCEDURE: IR-4(1) Assessment Objective Determine if the organization employs a Assessment Methods And Objects Examine: Incident response policy; pro Interview: Organizational personnel wi IR-4(CMS-1) – Enhancement (Modera Control Document relevant information related Applicability: All ASSESSMENT PROCEDURE: IR-4(CI	e organization.(Optional) port the incident handling process. References: ARS: IR-4(1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3; NIST 800-53/53A: IR-4(1) automated mechanisms to support the incident handling process. becedures addressing incident handling; automated mechanisms supporting incident handling; other relevant of th incident handling responsibilities.(Optional) to a security incident according to CMS Information Security Incident Handling and Breach Notification Proced References: ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	documents or records. edures.

 (i) the organization implements an incident handling capability for (ii) the incident handling capability is consistent with NIST SP 800 		alysis, containment, eradication, and recovery, and
Assessment Methods And Objects		
Examine: Incident response policy; procedures addressing incid incident is documented according to the CMS Information Securi		nents or records to determine if relevant information related to a securit
Interview: Organizational personnel with incident response traini CMS Information Security Incident Handling and Breach Notificat		prmation related to a security incident is documented according to the
R-4(CMS-2) – Enhancement (Moderate)		
Control		
	5 I	edia. Use sound forensics processes and utilities that support legal
Applicability: All References: A	ARS: IR-4(CMS-2); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	Related Controls:
ASSESSMENT PROCEDURE: IR-4(CMS-2).1		
Assessment Objective Determine if: (i) the organization implements an incident handling capability for (ii) the incident handling capability is consistent with NIST SP 800		alysis, containment, eradication, and recovery; and
Assessment Methods And Objects		
		nents or records to determine if evidence is preserved through technic utilities are used that support legal requirements. A chain of custody
		preserved through technical means, including secured storage of equirements. A chain of custody for forensic evidence is followed.
R-4(CMS-3) – Enhancement (Moderate)		
Control		
Identify vulnerability exploited during a security incident. Implem	ent security safeguards to reduce risk and vulnerability exploit	exposure.
Applicability: All References: A	ARS: IR-4(CMS-3); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	Related Controls:
ASSESSMENT PROCEDURE: IR-4(CMS-3).1		
Assessment Objective		
Determine if:		
 (i) the organization implements an incident handling capability for (ii) the incident handling capability is consistent with NIST SP 800 		alysis, containment, eradication, and recovery; and
Assessment Methods And Objects		and a second standard and the state of the
exploited during a security incident and security safeguards are in		nents or records to determine if the identification of vulnerabilities
	ing and operational responsibilities to determine if the identification	ation of vulnerabilities exploited during a security incident and security
R-5 – Incident Monitoring (Moderate)		
Control		
On-going monitoring of the CMS information system for security	security threats resulting from user, software, or hardware acti	I with system performance shall be monitored for the identification of ivity. All information system security incidents shall be tracked and
Suidance	bjeet to monitoring to verify compliance with this policy and to t	
It is good practice to separate system performance issues from in corruption in transmission within the system. Checksums or cycl safely relied upon to fully verify data correctness in the face of de	lic redundancy checks (CRCs) can help during the investigation eliberate (rather than random) changes.	changes can be the result of a security incident occurring or data n of these problems. While useful for error detection, CRCs cannot be ble to successfully exploit an RPC vulnerability they could gain comple

control over a remote computer. This would give the attacker the ability to take any action on the system that they want. For example, an attacker could change web pages, reformat the hard disk,

Applicability: All	References: ARS: IR-5; FISCAM: TAC-4.2; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#2.3; NIST 800-53/53A: IR-5; PISP: 4.8.5	Related Controls:
ASSESSMENT PROCEDURE: IR-5.1		
Assessment Objective		
	nd documents information system security incidents on an ongoing basis.	
Assessment Methods And Objects		
•	rocedures addressing incident monitoring; incident response records and documentation; other relevant documen	ts or records.
	with incident monitoring responsibilities.(Optional)	
Test: Incident monitoring capability for	r the organization.(Optional)	
IR-6 – Incident Reporting (Mode	erate)	
Control		
All IS incidents, or suspected incident	s, shall be reported to the CMS IT Service Desk (or equivalent organizational function) as soon as an incident con	nes to the attention of a user of CMS
information or information systems.	vents and confirmed security incidents by business partners shall also be reported to the CMS IT Service Desk in	accordance with established procedures.
Guidance		
The types of incident information repo	rted, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are	consistent with applicable laws, Executive
Orders, directives, policies, regulation	is, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer	Emergency Readiness Team (US-CERT) at
	sified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.	
reporting.	system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST S	P 800-61 provides guidance on incident
Applicability: All	References: ARS: IR-6; FISCAM: TAC-4.2; NIST 800-53/53A: IR-6; PISP: 4.8.6	Related Controls:
ASSESSMENT PROCEDURE: IR-6.1		Related Controls.
Assessment Objective		
Determine if:		
	ncident information to appropriate authorities;	
(ii) incident reporting is consistent with		
	eported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable	laws, Executive Orders, directives, policies,
regulations, standards, and guidance	and	
	the information system are reported to appropriate organizational officials in a timely manner to prevent security i	ncidents.
Assessment Methods And Objects		
	rocedures addressing incident reporting; NIST SP 800-61; incident reporting records and documentation; other re	levant documents or records.
Interview: Organizational personnel		
Test: Incident reporting capability for	the organization.(Optional)	
IR-6(1) – Enhancement (Moderate)		
Control		
	sist in the reporting of security incidents.	
	References: ARS: IR-6(1); NIST 800-53/53A: IR-6(1)	Related Controls:
ASSESSMENT PROCEDURE: IR-6(
Assessment Objective		
с , , , , , , , , , , , , , , , , , , ,	s automated mechanisms to assist in the reporting of security incidents.	
Assessment Methods And Objects		umanta ar recorde
		uments of records.
Examine: Incident response policy; p	rocedures addressing incident reporting; automated mechanisms supporting incident reporting; other relevant doc	
Examine: Incident response policy; p Interview: Organizational personnel	with incident reporting responsibilities.(Optional)	
Examine: Incident response policy; p Interview: Organizational personnel IR-7 – Incident Response Assist	with incident reporting responsibilities.(Optional)	
Examine: Incident response policy; p Interview: Organizational personnel IR-7 – Incident Response Assist Control	with incident reporting responsibilities.(Optional)	

Guidance		
Possible implementations of inci-	dent response support resources in an organization include a help desk or an assistance group an	id access to forensics services, when required.
Applicability: All	References: ARS: IR-7; NIST 800-53/53A: IR-7; PISP: 4.8.7	Related Controls:
ASSESSMENT PROCEDURE: IF	₹-7.1	
Assessment Objective		
Determine if:		
(i) the organization provides an i	ncident response support resource that offers advice and assistance to users of the information sy	stem for the handling and reporting of security incidents; and
(ii) the incident response suppor	t resource is an integral part of the organization's incident response capability.	
Assessment Methods And Obje	ects	
Examine: Incident response pol	icy; procedures addressing incident response assistance; other relevant documents or records.	
Interview: Organizational person	nnel with incident response assistance and support responsibilities.	
IR-7(1) – Enhancement (Modera	te)	
Control		
Employ automated mechanisms	to increase the availability of incident response-related information and support.	
Applicability: All	References: ARS: IR-7(1); NIST 800-53/53A: IR-7(1)	Related Controls:
ASSESSMENT PROCEDURE: IF	₹-7(1).1	
Assessment Objective		
· · · · · ·	plays automated machanisms to increase the availability of incident reasonable related information	and support for incident response support
Determine if the organization em	ploys automated mechanisms to increase the availability of incident response-related information a	
Determine if the organization em Assessment Methods And Obje		
Assessment Methods And Obje Examine: Incident response pol records.		dent response support and assistance; other relevant documents of

Interview: Organizational personnel with incident response support and assistance responsibilities and organizational personnel that require incident response support and assistance. (Optional)

Maintenance (MA) - Operational

MA-1 – System Maintenance Policy and Procedures (Moderate)

Control

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

Guidance

The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: MA-1; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-1; PISP: 4.9.1	Related Controls:

ASSESSMENT PROCEDURE: MA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents information system maintenance policy and procedures;

(ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review information system maintenance policy and procedures; and

(iv) the organization updates information system maintenance policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

ASSESSMENT PROCEDURE: MA-1.2

Assessment Objective

Determine if:

(i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-1(FIS-1) – Enhancement (Moderate)

Control

All system software is current, has current and complete documentation, and is still supported by the vendor.

Applicability: All	References: FISCAM: TSS-3.2.5, TSS-3.2.6	Related Controls:
ASSESSMENT PROCEDURE: MA-1(FIS-1).1	-	

Accessment Objective

Assessment Objective

Determine if the organization uses current system software with complete documentation and is vendor supported.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Interview: Management and systems programmers about the currency of system software, and the currency and completeness of software documentation.

Interview: System software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.

MA-2 – Controlled Maintenance (Moderate)

Control

Comprehensive maintenance procedures shall be developed, documented, and implemented effectively to conduct controlled periodic on-site and off-site maintenance of the CMS information

systems and of the physical plant within which these information systems reside. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS-approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly.

Guidance

All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Applicability: All; Optional for SS	References: /	ARS: MA-2; FISC	CAM: TSC-2.4.1, TSC-2.4.2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2,	Related Controls:	
	5.6.2.4#1.3; N	IST 800-53/53A:	: MA-2; PISP: 4.9.2		

ASSESSMENT PROCEDURE: MA-2.1

Assessment Objective

Determine if the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.

erganzatoriai por		
MA-2(1) – Enhancement (Mod	erate)	
Control		
Maintain maintenance records	s for each information system that includes:	
(a) Date and time of maintenal		
(b) Name of the individual perf	forming the maintenance, name of escort, if applicable,	
(c) Description of the maintena		
(d) List of equipment removed	l or replaced (including identification numbers, if applicable).	
Applicability: All	References: ARS: MA-2(1); FISCAM: TSC-2.4.3; NIST 800-53/53A: M/	A-2(1) Related Controls:
ASSESSMENT PROCEDURE:	: MA-2(1).1	
Assessment Objective		
		a of maintenances (ii) name of the individual performing the maintenances (iii)
-	maintains maintenance records for the information system that include: (i) the date and time	e of maintenance, (ii) name of the individual performing the maintenance, (iii)
Determine if the organization r	maintains maintenance records for the information system that include: (i) the date and time (iv) a description of the maintenance performed; and (v) a list of equipment removed or repla	
Determine if the organization r	(iv) a description of the maintenance performed; and (v) a list of equipment removed or repla	
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ot	 (iv) a description of the maintenance performed; and (v) a list of equipment removed or replace bjects 	laced (including identification numbers, if applicable).
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ot	(iv) a description of the maintenance performed; and (v) a list of equipment removed or repla bjects maintenance policy; procedures addressing controlled maintenance for the information sys	laced (including identification numbers, if applicable).
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ok Examine: Information system	(iv) a description of the maintenance performed; and (v) a list of equipment removed or repla bjects maintenance policy; procedures addressing controlled maintenance for the information sys	laced (including identification numbers, if applicable).
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ot Examine: Information system MA-2(FIS-1) – Enhancement (Control	(iv) a description of the maintenance performed; and (v) a list of equipment removed or repla bjects maintenance policy; procedures addressing controlled maintenance for the information sys	laced (including identification numbers, if applicable).
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ot Examine: Information system MA-2(FIS-1) – Enhancement (Control	(iv) a description of the maintenance performed; and (v) a list of equipment removed or replation of the maintenance performed; and (v) a list of equipment removed or replation bjects maintenance policy; procedures addressing controlled maintenance for the information sys (Moderate)	laced (including identification numbers, if applicable).
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ot Examine: Information system MA-2(FIS-1) – Enhancement (Control Flexibility exists in the data pro	(iv) a description of the maintenance performed; and (v) a list of equipment removed or repla bjects maintenance policy; procedures addressing controlled maintenance for the information sys (Moderate) occessing operations to accommodate regular and a reasonable amount of unscheduled maintenance References: FISCAM: TSC-2.4.4	laced (including identification numbers, if applicable). stem; maintenance records; other relevant documents or records.
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ok Examine: Information system MA-2(FIS-1) – Enhancement (Control Flexibility exists in the data pro Applicability: All	(iv) a description of the maintenance performed; and (v) a list of equipment removed or repla bjects maintenance policy; procedures addressing controlled maintenance for the information sys (Moderate) occessing operations to accommodate regular and a reasonable amount of unscheduled maintenance References: FISCAM: TSC-2.4.4	laced (including identification numbers, if applicable). stem; maintenance records; other relevant documents or records.
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ok Examine: Information system MA-2(FIS-1) – Enhancement (Control Flexibility exists in the data pro Applicability: All ASSESSMENT PROCEDURE: Assessment Objective	(iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced bjects maintenance policy; procedures addressing controlled maintenance for the information system (Moderate) occessing operations to accommodate regular and a reasonable amount of unscheduled maintenance regular and a reasonable amount o	laced (including identification numbers, if applicable). stem; maintenance records; other relevant documents or records. aintenance. Related Controls:
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ok Examine: Information system MA-2(FIS-1) – Enhancement (Control Flexibility exists in the data pro Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization a	(iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced bijects maintenance policy; procedures addressing controlled maintenance for the information sys (Moderate) occessing operations to accommodate regular and a reasonable amount of unscheduled maintenance References: FISCAM: TSC-2.4.4 : MA-2(FIS-1).1 accommodates regular and a reasonable amount of unscheduled maintenance in its data pro-	laced (including identification numbers, if applicable). stem; maintenance records; other relevant documents or records. aintenance. Related Controls:
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ok Examine: Information system MA-2(FIS-1) – Enhancement (Control Flexibility exists in the data pro Applicability: All ASSESSMENT PROCEDURE: Assessment Objective	(iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced bijects maintenance policy; procedures addressing controlled maintenance for the information system (Moderate) occessing operations to accommodate regular and a reasonable amount of unscheduled maintenance in the information system of the information system o	laced (including identification numbers, if applicable). stem; maintenance records; other relevant documents or records. aintenance. Related Controls:
Determine if the organization r name of escort, if necessary; (Assessment Methods And Ok Examine: Information system MA-2(FIS-1) – Enhancement (Control Flexibility exists in the data pro Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization a Assessment Methods And Ot	(iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced by a list of equipment removed or replaced by a maintenance policy; procedures addressing controlled maintenance for the information system (Moderate) Occessing operations to accommodate regular and a reasonable amount of unscheduled maintenance in the information system of the information system is the information of the information system of the information	laced (including identification numbers, if applicable). stem; maintenance records; other relevant documents or records. aintenance. Related Controls:

MA-2(FIS-2) – Enhancement (Moderate)		
Control		
a 11	software are scheduled to minimize the impact on operations and users thus allowing for adequate testing.	Advance notification on hardware changes is
given to users so that service is not unexpected		
Applicability: All	References: FISCAM: TSC-2.4.10, TSC-2.4.11	Related Controls:
ASSESSMENT PROCEDURE: MA-2(FIS-2).	1	
Assessment Objective		
Determine if:		
(i) the organization schedules hardware equip	ment and related software changes such to minimize user impact and maximize resources for adequate te	sting; and
(ii) the organizational advance notification for	hardware equipment changes does not cause unexpected interrupted user services.	
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation.		
Interview: Senior management, data process	ing management, and user management.	
MA-2(PII-1) – Enhancement (Moderate)		
Control		
In facilities where PII is stored or accessed, de	ocument repairs and modifications to the physical components of a facility which are related to security (for	
Applicability: All	References: HIPAA: 164.310(a)(2)(iv)	Related Controls:
ASSESSMENT PROCEDURE: MA-2(PII-1).1	1	
Assessment Objective		
	irs and modifications to the facility containing PII.	
Assessment Methods And Objects		
	or plan and elevation drawings) are updated when repairs and modifications cause changes to the physica	components of the facility containing PII
, , , , , , , , , , , , , , , , , , ,	lity management responsibilities, to determine if facility documents reflect security changes caused by rep	, , , ,
	nine if repairs or modifications document physical security implications when the facility is protecting PII.	
MA-3 – Maintenance Tools (Moderate		
Control		
	ng diagnostic and test equipment and administration utilities, shall be approved, controlled, and monitored.	Approved tools shall be maintained on an on-
going basis.		· · · · · · · · · · · · · · · · · · ·
Guidance		
	re and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardwa	are or software packet sniffer that is
The intent of this control is to address hardwa	re and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardwantenance activity). Hardware and/or software components that may support information system maintenance	are or software packet sniffer that is e, yet are a part of the system (e.g., the
The intent of this control is to address hardwa introduced for the purpose of a particular mair	ntenance activity). Hardware and/or software components that may support information system maintenance or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by t	e, yet are a part of the system (e.g., the
The intent of this control is to address hardwa introduced for the purpose of a particular mair	ntenance activity). Hardware and/or software components that may support information system maintenance	e, yet are a part of the system (e.g., the
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "ls," "ipconfig,"	ntenance activity). Hardware and/or software components that may support information system maintenance or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by t	e, yet are a part of the system (e.g., the his control.
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "ls," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1	ntenance activity). Hardware and/or software components that may support information system maintenance or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by t	e, yet are a part of the system (e.g., the his control.
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "Is," "ipconfig," Applicability: All	ntenance activity). Hardware and/or software components that may support information system maintenance or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by t	e, yet are a part of the system (e.g., the his control.
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "ls," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective Determine if:	ntenance activity). Hardware and/or software components that may support information system maintenance or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by t	e, yet are a part of the system (e.g., the his control.
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "ls," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective Determine if:	onitors the use of information system maintenance tools; and	e, yet are a part of the system (e.g., the his control.
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "ls," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective Determine if: (i) the organization approves, controls, and main (ii) the organization maintains maintenance to	onitors the use of information system maintenance tools; and	e, yet are a part of the system (e.g., the his control.
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "Is," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective Determine if: (i) the organization approves, controls, and me (ii) the organization maintains maintenance to Assessment Methods And Objects	onitors the use of information system maintenance tools; and ols on an ongoing basis.	e, yet are a part of the system (e.g., the his control. Related Controls:
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "Is," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective Determine if: (i) the organization approves, controls, and me (ii) the organization maintains maintenance to Assessment Methods And Objects	onitors the use of information system maintenance tools; and ols on an ongoing basis.	e, yet are a part of the system (e.g., the his control. Related Controls:
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "Is," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective Determine if: (i) the organization approves, controls, and mo (ii) the organization maintains maintenance to Assessment Methods And Objects Examine: Information system maintenance particular	onitors the use of information system maintenance tools; and ols on an ongoing basis.	e, yet are a part of the system (e.g., the his control. Related Controls:
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "Is," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective Determine if: (i) the organization approves, controls, and me (ii) the organization maintains maintenance to Assessment Methods And Objects Examine: Information system maintenance por records; other relevant documents or records.	onitors the use of information system maintenance tools; and ols on an ongoing basis.	e, yet are a part of the system (e.g., the his control. Related Controls:
The intent of this control is to address hardwa introduced for the purpose of a particular mair software implementing "ping," "Is," "ipconfig," Applicability: All ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective Determine if: (i) the organization approves, controls, and main (ii) the organization maintains maintenance to Assessment Methods And Objects Examine: Information system maintenance pur records; other relevant documents or records. MA-4 – Remote Maintenance (Modera Control	onitors the use of information system maintenance tools; and ols on an ongoing basis.	e, yet are a part of the system (e.g., the his control. Related Controls: ation system maintenance tools; maintenance

The use of remote diagnostic tools shall be described in the SSP for the information system. Maintenance records for all remote maintenance, diagnostic, and service activities shall be maintained and shall be reviewed periodically by appropriate organization officials. All sessions and remote connections shall be terminated after the remote maintenance is completed. If password-based authentication is used during remote maintenance, the passwords shall be changed following each remote maintenance service.

Guidance

Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST SP 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdq.cfm.

County rigency provides a nating of approved in	nedia samazation predecto at http://www.ned.gev/na/geveniment/mag.onm.	
Applicability: All	References: ARS: MA-4; FISCAM: TAC-2.1.3; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4; PISP: 4.9.4	Related Controls: IA-2, MP-6
ASSESSMENT PROCEDURE: MA-4.1		
Assessment Objective		
Determine if the organization authorizes, monito	rs, and controls remotely executed maintenance and diagnostic activities, if employed.	
Assessment Methods And Objects		
	cy; procedures addressing remote maintenance for the information system; information system design do	cumentation; information system
5 5	ation; maintenance records; other relevant documents or records.	
Interview: Organizational personnel with information	ation system maintenance responsibilities.	
MA-4(1) – Enhancement (Moderate)		
Control		
	ure that appropriate information security personnel review the maintenance records of the remote session	
Applicability: All	References: ARS: MA-4(1); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4(1)	Related Controls:
ASSESSMENT PROCEDURE: MA-4(1).1		
Assessment Objective		
Determine if:		
(i) the organization audits all remote maintenanc	•	
(ii) designated organizational personnel review the	he maintenance records of remote sessions.	
Assessment Methods And Objects		
	cy; procedures addressing remote maintenance for the information system; maintenance records; audit re	ecords; other relevant documents or records.
Interview: Organizational personnel with information	ation system maintenance responsibilities.	
MA-4(2) – Enhancement (Moderate)		
Control		
Document the use of remote diagnostic tools in t		
Applicability: All	References: ARS: MA-4(2); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-4(2)	Related Controls:
ASSESSMENT PROCEDURE: MA-4(2).1		
Assessment Objective		
	allation and use of remote maintenance and diagnostic links in the security plan for the information system	m.
Assessment Methods And Objects		
Examine: Information system maintenance polic other relevant documents or records.	cy; procedures addressing remote maintenance for the information system; information system security p	lan; maintenance records; audit records;

MA-4(CMS-1) – Enhancement (Moderate)		
Control		
	by the CIO or his/her designated representative:	
	ns; utilize strong identification and authentication techniques, such as tokens; and when remote mainten	
	entication is used during remote maintenance, change the passwords following each remote maintenance	
	References: ARS: MA-4(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: MA-4(CMS-1).1	
Assessment Objective		
•	itors, and controls remotely executed maintenance and diagnostic activities, if employed.	
Assessment Methods And Objects		
designated representative: diagnostic commu completed, all sessions and remote connectio maintenance service. Interview: Organizational personnel with info representative: diagnostic communications ar	blicy and procedures; other relevant documents or records to determine that remote maintenance is auth nications are encrypted / decrypted; utilize strong identification and authentication techniques, such as to ns are terminated. If password-based authentication is used during remote maintenance, the passwords mation system maintenance responsibilities to determine that remote maintenance is authorized in writin e encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and w	kens; and when remote maintenance is are changed following each remote ng by the CIO or his/her designated when remote maintenance is completed, all
	ted. If password-based authentication is used during remote maintenance, the passwords are changed to	following each remote maintenance service.
MA-5 – Maintenance Personnel (Mode	erate)	
Control		
Maintenance personnel procedures shall be d maintenance on the information system shall	eveloped, documented, and implemented effectively to control maintenance of CMS information systems be maintained.	s. A list of individuals authorized to perform
Guidance		
organizational information or could result in a	naintenance locally or remotely) have appropriate access authorizations to the information system when future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have r ons supervise maintenance personnel during the performance of maintenance activities on the informatic	needed access authorizations, organizationa
Applicability: All	References: ARS: MA-5: NIST 800-53/53A: MA-5: PISP: 4.9.5	Related Controls:
ASSESSMENT PROCEDURE: MA-5.1		
Assessment Objective		
	orized personnel to perform maintenance on the information system.	
Assessment Methods And Objects	onzed personner to perform maintenance on the information system.	
	plicy; procedures addressing maintenance personnel; service provider contracts and/or service level agre	ements: list of authorized personnel:
maintenance records; other relevant documer		
Interview: Organizational personnel with info		
MA-5(0) – Enhancement (Moderate)		
Control		
	form maintenance. Ensure maintenance personnel have appropriate access authorizations to the inform	ation system when maintenance activities a
	se maintenance personnel during the performance of maintenance activities when they do not have the r	
Applicability: All	References: ARS: MA-5(0); HIPAA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: MA-5; PISP: 4.9.5	Related Controls:
ASSESSMENT PROCEDURE: MA-5(0).1		
Assessment Objective	amonte co anacified in the baseline control and the anacific CMC requirements or anocarily dis this amon	lifting opportunity to the booking control
	ements as specified in the baseline control and the specific CMS requirements as prescribed in this amp	biliging enhancement to the baseline control
Assessment Methods And Objects		in the second
Examine: information system maintenance p	plicy; procedures addressing maintenance personnel; service provider contracts and/or service level agree	eements; list of authorized personnel;

maintenance records; other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities.

Control Maintenance services and practice bit determine the priority of each system based on the criticality of the system for continued business operations. Each system should be prioritized and interconnections between each of the enterprises systems mapped and dataflow dagrams developed. Next maintenance contracts are will as emergency provider contracts and/or service level agreements; inventory and spare parts for the organization-defined term paried of failure. Assessment Objective Examine: Information system maintenance for the information system; proculture addressing flow maintenance for the information system; maintenance for the information system; service provider contracts and/or service level agreements; inventory and maintenance for the information system; maintenance for the information system; proculture addressing flow maintenance for the information system; flow flow sys			
Maintenance services and parts shall be available in a timely manner. Guidance R is good practice to determine the priority of each system based on the criticality of the system for continued business operations. Each system should be prioritized and interconnections between each of the enterprise's system magned and datafield valagrams developed. Next maintenance contracts as well as emergency maintenance considerations will determine needed availability and pre-placement of spare parts. Related Controls: Assessment Objective References: ARS: MA-6; NIST 800-83/53:: MA-6; PISP: 4.9.6 Related Controls: Assessment Objective Determine If: (i) the organization defines the time period within which support and spare parts must be obtained after a failure; and (iii) the organization-defined time period of failure. Assessment Objective Determine If: (iii) the organization defines the time period within which support and spare parts for the organization-defined time period of failure. Assessment Objective Control Control Control Control Control Control is objective Control is objective Objective Determine If: Notrol (Not Critical systems and applications (including Major Applications (MA) and General Support Systems (SSS) and their components) within twent Application approximation system maintenance support and spare parts. Notrol (Not Critical systems and applications (Including Major Applications) Related Controls: <td>MA-6 – Timely Maintenance (Moderate)</td> <td></td> <td></td>	MA-6 – Timely Maintenance (Moderate)		
Guidance End of practice to determine the priority of each system based on the criticality of the system for continued business operations. Each system should be prioritized and interconnections between each of the enterprise's systems mapped and dataflow diagrams developed. Next maintenance constraines well as emergence ymaintenance considerations will determine needed availability and pre-placement of spare parts. Applicability: All References: ARS: MA-6; NIST 800-53553; MA-6; PISP; 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6.1 Assessment Objective Determine) f: I) the organization defines key information system components: (ii) the organization-defined tist of key information system components within the organization-defined time period of failure. Assessment Methods And Objects Examine: Information system maintenance of the information system service provider contracts and/or service level agreements: inventory and value parts for CMS critical system maintenance for the information system; service provider contracts and/or service level agreements: inventory and value of tailure. Assessment Methods And Objects References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53/; MA-6; PISP: 4.9.6 Related Controls: Control Obtain maintenance oplicy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and values of tailure. Assessment Objective Related Controls: ASSESSMENT PROCEDURE: MA-6(0); Related Controls: ASSESSMENT PROCEDURE: MA-6(0	Control		
It is good practice to determine the priority of each system based on the critically of the system for continued business operations. Each system should be prioritized and interconnections between each of the controls is an entryprised system in mapped and dataflow dagrams developed. Next maintenance contracts as well as emergency maintenance considerations will determine needed availability and pre-placement of spare parts. Related Controls: Assessment Objective Determine if. Iterformation system components: Iterformation system components: (i) the organization defines the time period within which support and spare parts must be obtained after a failure; and Iterformation system components: Iterformation system components: (ii) the organization defines the time period within which support and spare parts must be obtained after a failure; and Iterformation system controls and/or service level agreements: inventory and availability of gare parts. Assessment Methods And Objects Examine: information system maintenance support and spare parts for CMS critical systems and applications. Iterformation system service provider contracts and/or service level agreements: inventory and availability of gare parts. Information system service provider contracts and/or service level agreements: inventory and availability of spare parts. Related Controls: Assessment Objective References: ARS: MA-6(0); FISCAM: TSC-2.4.5, NIST 800-53/3A: MA-6; PISP.4.9.6 Related Controls: Assessment Motiods and Objects References: ARS: MA-6(0); FISCAM: TSC-2.4.5, NIST 800-53/3A: MA-6; PISP.4	Maintenance services and parts shall be available	e in a timely manner.	
each of the enterprise's systems mapped and dataflow diagrams developed. Not maintenance considerations will as emergency maintenance considerations will determine needed availability and pre-placement of spare parts. Applicability: Al References: ARS: MA-6; NIST 800-53/53: MA-6; PISP: 4.9.6 Research of the organization defines here information system components; (i) the organization defines here information system components; (ii) the organization defines here information system components; (ii) the organization defines here information system components; (ii) the organization defines here information system components; (iii) the organization defines here information system components; (ivertify) and the organization defines here information system components; (ivertify) and the organization defines here there information system components in displays and applications; Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control and the specific C			
Applicability: All References: ARS: MA-6; NIST 800-53/53/s: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-61 ASSESSMENT CODEcima in the imperiod within which support and spare parts must be obtained after a failure; and (i) the organization defines key information system components; (i) the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period within which support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure. Assessment Underdot AD Objects Examine: information system maintenance policy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance responsibilities. MA-6(0) = Enhancement (Moderate) Examine: information system service provider contracts and/or service level agreements; inventory and systems (CSS) and their components) within twent four (24) hours of failure. Related Controls: Assessment Objective References: ARS: MA-6(0); FISCAM: TSC-24.5, NIST 800-53/53/a: MA-6; PISP: 4.9.6 Related Controls: Assessment Methods And Objects Related Controls: Related Controls: Assessment Objective Control Related Controls: Related Controls: Related Controls: Assessament Objective Related Controls:<	each of the enterprise's systems mapped and da	taflow diagrams developed.	be prioritized and interconnections between
ASSESSMENT PROCEDURE: MA-6.1 Assessment Methods And Objectiv Assessment Methods And Objectiv Support and spare parts must be obtained after a failure: and (i) the organization defines key information system captors and spare parts of the organization-defined list of key information system captors and/spare parts information system maintenance policy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements: inventory and availability of spare parts; information system maintenance responsibilities. MA-500_Enhancement (Moderate) Control Control Sassessment Objective Assessment Objective References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 600-53/53A: MA-6; PISP: 4.9.6 Related Controls: Assessment Objective Assessment Objective References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 600-53/53A: MA-6; PISP: 4.9.6 Related Controls: Assessment Objective Determine if the organization dense to requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancements: inventory and availability of spare parts; information system maintenance policy: procedures addressing timely maintenance for the information system: service provider contracts and/or service level agreements: inventory and availability of spare parts; information system servicity fluin (for organization-defined list of key information system: service provider contracts and/or service level agreements: inventory and availability of spare parts; information system service provedures addressing timely m			Related Controls:
Assessment Objective Determine if: (i) the organization defines key information system components: (ii) the organization obtains maintenance support and spare parts must be obtained after a failure; and (iii) the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure. Assessment Methods And Objects Examine: Information system maintenance policy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance responsibilities. MA:6(0) = Enhancement (Moderate) References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 ASSESSMENT PROCEDURE: MA-6(0.1) References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 ASSESSMENT PROCEDURE: MA-6(0.1) References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 ASSESSMENT PROCEDURE: MA-6(0.1) References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and valiability of spare parts; information system maintenance responsibilities. MA:CONS-1 - Off-site Physical Reparts of Systems (Moderate) Control	•••		
Determine f. Comparization defines the time period within which support and spare parts must be obtained after a failure; and Comparization defines the time period within which support and spare parts for the organization-define time period of failure. Assessment Methods And Objects Examine: Information system maintenance support and spare parts for the organization-define time period of failure. Assessment Methods And Objects Examine: Information system maintenance support and spare parts information system maintenance treeponsibilities. MA-6(0) – Enhancement (Moderate) Control Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Assessment Objective References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: Assessment Objective Detain maintenance support and spare parts for CMS critical systems and applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Assessment Objective References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: Assessment Objective Determine if the organization-defined list of key information system components and organization-defined list of key information system components and organization-defined list of key information system maintenance for the information system maintenance prelase system should co			
I) the organization defines key information system components: IIII the organization defines key information system to be the imperiod within which support and spare parts must be obtained after a failure; and IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	•		
(ii) the organization defines the time period within which support and spare parts must be obtained after a fallure; and (iii) the organization defines the time period within which support and spare parts for the organization-defined list of key information system components within the organization-defined me period of failure. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance responsibilities. MA-6(0) – Enhancement (Moderate) Control Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Assessment Dejective Detarmine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance responsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Control Control Control shall be dev		n components:	
(iii) the organization obtains maintenance support and spare parts for the organization-defined list of key information system; service provider contracts and/or service level agreements; inventory and availability of spare parts. Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts. Information system maintenance responsibilities. MA-6(0) = Enhancement (Moderate) Control Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Applicability: All References: ARS: MA-6(0); FISCAM: TSC-24.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0.1) References: arRS: MA-6(0); FISCAM: TSC-24.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0.1) References: arRS: MA-6(0); FISCAM: TSC-24.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0.1) References: arRS: MA-6(0); FISCAM: TSC-24.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0.1) References: arRS: MA-6(0); FISCAM: TSC-24.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0.1) References: ARS: MA-6(0.1); FISCAM: information system maintenance policy; procedures addressing timply maintenance policy info			
Assessment Methods And Objects Examine: Information system maintenance policy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance responsibilities. MA-6(0) = Enhancement (Moderate) Control Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Assessment Objective Assessment Information system maintenance policy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance policy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system			anization-defined time period of failure.
Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance responsibilities. MA-6(0) – Enhancement (Moderate) Control Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (SSS) and their components) within twent four (24) hours of failure. Applicability: All References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0).1 Assessment Objective Related Controls: Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control and the specific CMS requirements as prescribed in this amplifying enhancements; inventory and availability of spare parts; information system maintenance responsibilities. MA-CMS-1 - Off-site Physical Repair of Systems (Moderate) Control Control Control shall be developed, documented, and implemented effectively to enable off-site physical repair of system swithout compromising security functionality. Related Controls: AC-19(CMS-1), AC-3 MA-CMS-1 Control Control Control shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising securi			
availability of spare parts; information system security plan; other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-6(0) – Enhancement (Moderate) Control Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Applicability: All References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0.1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system; components and organization-defined time period within which support and spare parts must be obtained after a failure): other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired System should match the appro- Change Management Deseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Control		y; procedures addressing timely maintenance for the information system; service provider contracts an	d/or service level agreements; inventory and
MA-6(0) - Enhancement (Moderate) Control Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Applicability: All References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0).1 Assessment Objective Related Controls: Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance reponsibilities. MA-CMS-1 ~ Off-site Physical Repair of Systems (Moderate) Control Control Control shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Related Controls: AC-19(CMS-1), AC-3			
Control Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Applicability: All References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSEMENT PROCEDURE: MA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance responsibilities. MA-CMS-1 - Off-Site Physical Repair of Systems (Moderate) Control Control Control Control References: ARS: MA-6(NS-1; PISP: 4.9.7 Related Controls: Assessment Objective Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted m	Interview: Organizational personnel with information	tion system maintenance responsibilities.	
Obtain maintenance support and spare parts for CMS critical systems and applications (including Major Applications (MA) and General Support Systems (GSS) and their components) within twent four (24) hours of failure. Applicability: All References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0).1 Assessment Objective Related Controls: Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance reponsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Control Control shall be developed, documented, and implemented effectively to enable off-site physical repair of system swithout compromising security functionality or confidentiality. Guidance References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) Assessment between the approxemation and proper level and system before it is put back into operation when the system has returned from off-site repair. The repaired system sho	MA-6(0) – Enhancement (Moderate)		
four (24) hours of failure. References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance records. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Control Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. References: ARS: MA-CMS-1; PISP: 4.9.7 Assessment Objective Determine the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment the organization effectively develops procedures; other relevant docu	Control		
Applicability: All References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6 Related Controls: ASSESSMENT PROCEDURE: MA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy: procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts; inventory and documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-CMS-1 - Off-site Physical Repair of Systems (Moderate) Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of system swithout compromising security functionality or confidentiality. Guidance References: ARS: MA-CMS-1; PISP: 4.9.7 It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. References: ARS: MA-CMS-1; PISP: 4.9.7 Assessment Objective <t< td=""><td>Obtain maintenance support and spare parts for</td><td>CMS critical systems and applications (including Major Applications (MA) and General Support System</td><td>s (GSS) and their components) within twenty-</td></t<>	Obtain maintenance support and spare parts for	CMS critical systems and applications (including Major Applications (MA) and General Support System	s (GSS) and their components) within twenty-
ASSESSMENT PROCEDURE: MA-6(0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system records. Interview: Organization-defined list of key information system components and organization-defined time period within which support and spare parts must be obtained after a failure); other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-CMS-1 Off-site Physical Repair of Systems (Moderate) Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organization effectively develops procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair.	four (24) hours of failure.		
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts; use be obtained after a failure); other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-CMIS-1 — Off-site Physical Repair of Systems (Moderate) Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) ASSESSMENT PROCEDURE: MA-CMS-1.1 Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organization approach and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organization approach and procedures; other relevant documents or records to determine that only authorized personne	Applicability: All	References: ARS: MA-6(0); FISCAM: TSC-2.4.5; NIST 800-53/53A: MA-6; PISP: 4.9.6	Related Controls:
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system maintenance responsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. CP-9, SC-12(CMS-1), AC-3 CP-9,	ASSESSMENT PROCEDURE: MA-6(0).1		
Assessment Methods And Objects Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts must be obtained after a failure); other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Researce of the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Objective Determine if the organization effectively develops procedures; other relevant documents or records to determine that only authorized personnel are permitted access to system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Assessment Objective		
Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts; information and inplemented after a failure); other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Control Control complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 References: ARS: MA-CMS-1; PISP: 4.9.7 References: ARS: MA-CMS-1; PISP: 4.9.7 Cassessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to systems during off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Determine if the organization meets the requirem	ents as specified in the baseline control and the specific CMS requirements as prescribed in this ampli	fying enhancement to the baseline control.
availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts must be obtained after a failure); other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Control shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) Assessment Objective Determine if the organization effectively develops procedures, occurrents procedures, and implements of records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organization al personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Assessment Methods And Objects		
availability of spare parts; information system security plan (for organization-defined list of key information system components and organization-defined time period within which support and spare parts must be obtained after a failure); other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Control shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) Assessment Objective Determine if the organization effectively develops procedures, occurrents procedures, and implements of records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organization al personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Examine: Information system maintenance polic	y; procedures addressing timely maintenance for the information system; service provider contracts an	d/or service level agreements; inventory and
Interview: Organizational personnel with information system maintenance responsibilities. MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 ASSESSMENT PROCEDURE: MA-CMS-1.1 Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	availability of spare parts; information system set	curity plan (for organization-defined list of key information system components and organization-defined	time period within which support and spare
MA-CMS-1 – Off-site Physical Repair of Systems (Moderate) Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 (C-9, SC-12(CMS-1)) Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.			
Control Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.			
Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality. Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Resetted Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) ASSESSMENT PROCEDURE: MA-CMS-1.1 Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	MA-CMS-1 – Off-site Physical Repair of	Systems (Moderate)	
Guidance It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) ASSESSMENT PROCEDURE: MA-CMS-1.1 References: a RS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Control		
It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approx Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) ASSESSMENT PROCEDURE: MA-CMS-1.1 Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Controls shall be developed, documented, and ir	nplemented effectively to enable off-site physical repair of systems without compromising security funct	ionality or confidentiality.
Change Management baseline. Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 ASSESSMENT PROCEDURE: MA-CMS-1.1 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Guidance		
Storage media control when encrypted may take special considerations. Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) ASSESSMENT PROCEDURE: MA-CMS-1.1 Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.		ew of a system before it is put back into operation when the system has returned from off-site repair. T	he repaired system should match the approved
Applicability: All References: ARS: MA-CMS-1; PISP: 4.9.7 Related Controls: AC-19(CMS-1), AC-3 CP-9, SC-12(CMS-1) ASSESSMENT PROCEDURE: MA-CMS-1.1 Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising scurity functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Change Management baseline.		
ASSESSMENT PROCEDURE: MA-CMS-1.1 ASSESSMENT Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.			
ASSESSMENT PROCEDURE: MA-CMS-1.1 Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	Applicability: All	Keterences: AKS: MA-UMS-1; PISP: 4.9.7	
Assessment Objective Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	ASSESSMENT BROCEDURE, MA CMS 4.4		UF-9, 3U-12(UNIO-1)
Determine if the organization effectively develops procedures, documents procedures, and implements off-site repair of systems without compromising security functionality or confidentiality. Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.			
Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.		and a first state of the second descent of the second of the second state of the second sta	
Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorized personnel are permitted access to the system for off-site repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.		procedures, documents procedures, and implements off-site repair of systems without compromising	security functionality or confidentiality.
repair. Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.	-		and the second
Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel are permitted access to systems during off-site repair.		y and procedures; other relevant documents or records to determine that only authorized personnel are	e permitted access to the system for off-site
	•	tion system maintenance responsibilities to determine that only authorized personnel are permitted ac	case to systems during off-site repair
Rev. 9 Page 95 of 189 BPSSM Appendix A, Attachmer	Rev. 9	Page 95 of 189	BPSSM Appendix A, Attachment 2

MA-CMS-1(CMS-0) – Enhancement (Moderate)	
Control	
Access to system for repair must be by authorized personnel only. Storage media must be removed before shipment for repairs. Unusa	able storage media must be degaussed or destroyed by
authorized personnel. After maintenance is performed, check security features to verify they are functioning properly.	Deleted Controlog
Applicability: All References: ARS: MA-CMS-1(CMS-0); HIPAA: 164.310(d)(2)(i)	Related Controls:
ASSESSMENT PROCEDURE: MA-CMS-1(CMS-0).1	
Assessment Objective	
Determine if the organization allows only authorized personnel perform maintenance on the information system.	
Assessment Methods And Objects	
Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorize Storage media must be removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized p are checked to verify they are functioning properly.	ed personnel are permitted access to the system for repair. personnel. After maintenance is performed, security features
Interview: Organizational personnel with information system maintenance responsibilities determine that only authorized personnel are	permitted access to system for repair. Storage media must be
removed before shipment for repairs. Unusable storage media must be degaussed or destroyed by authorized personnel. After mainter	nance is performed, security features are checked to verify
they are functioning properly.	
MA-CMS-2 – On-site Physical Repair of Systems (Moderate)	
Control	
Controls shall be developed, documented, and implemented effectively to enable on-site physical repair of systems without compromisin	ng security functionality or confidentiality.
Guidance	
It is good practice to complete a full security review of a system before it is put back into operation when the system has completed repa Management baseline.	irs. The repaired system should match the approved Change
Storage media control when encrypted may take special considerations.	
Applicability: All References: ARS: MA-CMS-2; PISP: 4.9.8	Related Controls: AC-19(CMS-1), AC-3, CP-9, SC-12(CMS-1)
ASSESSMENT PROCEDURE: MA-CMS-2.1	
Assessment Objective	
Determine if the organization effectively develops procedures, documents procedures, and implements on-site repair of systems without	compromising security functionality or confidentiality.
Assessment Methods And Objects	
Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorize repair.	ed personnel are permitted access to the system for on-site
Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel a	re permitted access to systems during on-site repair.
MA-CMS-2(CMS-1) – Enhancement (Moderate)	
Control	
Access to system for repair must be by authorized personnel only.	
Applicability: All References: ARS: MA-CMS-2(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: MA-CMS-2(CMS-1).1	
Assessment Objective	
Determine if the organization allows only authorized personnel perform maintenance on the information system.	
Determine it the organization allows only authorized personnel perform maintenance on the information system.	
Assessment Methods And Objects	
Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorize	
Assessment Methods And Objects	
Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorize	
Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorize Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel per	
Assessment Methods And Objects Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that only authorize Interview: Organizational personnel with information system maintenance responsibilities to determine that only authorized personnel personnel personnel MA-CMS-2(CMS-2) – Enhancement (Moderate)	

ASSESSMENT PROCEDURE: MA-CMS-2(CMS-2).1

Assessment Objective

Determine if the organization performs physical repair of servers within protected environments.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine physical repair of servers is performed within protected environments. **Interview:** Organizational personnel with information system maintenance responsibilities to determine physical repair of servers is performed within protected environments.

Media Protection (MP) – Operational

Wedia Protection (WP) - Operation	niai	
MP-1 - Media Protection Policy and Pro	cedures (Moderate)	
Control		
	, documented, and implemented effectively to address media access; media labeling; media transpor	: media destruction: media sanitization and
	a records. The MP procedures shall be consistent with applicable laws, Executive Orders, directives	
Guidance		
The media protection policy and procedures are	consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and gu	idance. The media protection policy can be
included as part of the general information secu	rity policy for the organization. Media protection procedures can be developed for the security program	n in general, and for a particular information
system, when required. NIST SP 800-12 provide	es guidance on security policies and procedures.	
Applicability: All	References: ARS: MP-1; FISCAM: TAC-3.4; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1; NIST 800-53/53A: MP-1; PISP: 4.10.1	Related Controls:
ASSESSMENT PROCEDURE: MP-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and documents me	edia protection policy and procedures;	
	on policy and procedures to appropriate elements within the organization;	
	eriodically review media protection policy and procedures; and	
	olicy and procedures when organizational review indicates updates are required.	
Assessment Methods And Objects		
Examine: Media protection policy and procedur		
Interview: Organizational personnel with inform	ation system media protection responsibilities.(Optional)	
ASSESSMENT PROCEDURE: MP-1.2		
Assessment Objective		
Determine if:		
(i) the media protection policy addresses purpos	e, scope, roles and responsibilities, management commitment, coordination among organizational er	tities, and compliance;
(ii) the media protection policy is consistent with	the organization's mission and functions and with applicable laws, directives, policies, regulations, st	andards, and guidance; and
(iii) the media protection procedures address all	areas identified in the media protection policy and address achieving policy-compliant implementatio	ns of all associated security controls.
Assessment Methods And Objects		
Examine: Media protection policy and procedur		
	ation system media protection responsibilities.(Optional)	
MP-1(PII-1) – Enhancement (Moderate)		
Control		
Semiannual inventories of magnetic tapes conta	ining PII are conducted. The organization accounts for any missing tape containing PII by documenti	ng the search efforts and notifying the tape
initiator of the loss.		- · · · ·
Applicability: All	References: IRS-1075: 3.2#3.2, 3.2#3.3	Related Controls:
ASSESSMENT PROCEDURE: MP-1(PII-1).1		
Assessment Objective		
Determine if:		
(i) the organization verifies semiannual inventor		
	be containing PII by documenting the search efforts and notifying the tape initiator of the loss.	
Assessment Methods And Objects		
Examine: Records of semiannual inventories of	PII magnetic tapes conducted. If tapes are missing the initiator is notified and a record of the investi	gation is documented.
MP-2 – Media Access (Moderate)		
Control		
Procedures shall be developed, documented, and	nd implemented effectively to ensure adequate supervision of personnel and review of their activities	o protect against unauthorized receipt, change
Examine: Records of semiannual inventories of P-2 – Media Access (Moderate)		gation is documented.

access attempts and access granted.

access allempts and access granted.		
Guidance		
Information system media includes both digital m	nedia (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks	, digital video disks) and non-digital media
	to portable and mobile computing and communications devices with information storage capability (e.g.,	notebook computers, personal digital
assistants, cellular telephones).		vientions, de surrent in melleur and muse dumes
An organizational assessment of risk guides the	selection of media and associated information contained on that media requiring restricted access. Orga a authorized to access the media, and the specific measures taken to restrict access. The rigor with which	hizations document in policy and procedures,
	nation contained on the media. For example, fewer protection measures are needed for media containing	
to be in the public domain, to be publicly releasa	ble, or to have limited or no adverse impact on the organization or individuals if accessed by other than a	authorized personnel. In these situations, it is
	e the media resides provide adequate protection.	
Applicability: All	References: ARS: MP-2; FISCAM: TAC-3.1.A.6, TAY-4.1.1; HIPAA: 164.308(a)(3)(ii)(A),	Related Controls:
	164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1; NIST 800-53/53A: MP-2; PISP: 4.10.2	
ASSESSMENT PROCEDURE: MP-2.1		
Assessment Objective		
Determine if the organization restricts access to	information system media to authorized users.	
Assessment Methods And Objects		
	policy; procedures addressing media access; access control policy and procedures; physical and environ	mental protection policy and procedures;
media storage facilities; access control records;		
Interview: Organizational personnel with information	ation system media protection responsibilities.	
MP-2(1) – Enhancement (Moderate)		
Control		
Employ automated mechanisms to restrict acces	is to media storage areas and to audit access attempts and access granted.	
Guidance		
	to designated media storage areas within an organization where a significant volume of media is stored	and is not intended to apply to every location
where some media is stored (e.g., in individual o		T
Applicability: All	References: ARS: MP-2(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.5; IRS-1075: 4.6#1; NIST 800-53/53A:	Related Controls:
ASSESSMENT PROCEDURE: MP-2(1).1	MP-2(1)	
Assessment Objective		
Determine if:		
	sms to restrict access to media storage areas; and	
	isms to audit access attempts and access granted.	
Assessment Methods And Objects		
	policy; procedures addressing media access; access control policy and procedures; physical and environ	mental protection policy and procedures:
	access control records; audit records; other relevant documents or records.	
Test: Automated mechanisms implementing acc	ess restrictions to media storage areas.(Optional)	
MP-3 – Media Labeling (Moderate)		
Control		
Storage media and information system output sh	all have external labels affixed to indicate the distribution limitations, applicable security classification, ar	nd handling caveats of the information.
Specific types of media or hardware components	s may be exempted from the labeling requirement, so long as the exempted items remain within a secure	environment. Only the CIO or his/her
designated representative shall have the authorit	ty to exempt specific types of media or hardware components from the labeling requirement.	
Guidance		
An organizational assessment of risk guides the	selection of media requiring labeling. Organizations document in policy and procedures, the media requi	ring labeling and the specific measures taken
	is control is applied is commensurate with the FIPS 199 security categorization of the information contain	ned on the media. For example, labeling is not
	ined by the organization to be in the public domain or to be publicly releasable.	Delete I Oceanies
Applicability: All	References: ARS: MP-3; IRS-1075: 4.6#1, 5.1#1.2, 5.3#2.1-2, 5.3#3; NIST 800-53/53A: MP-3; PISP: 4.10.2	Related Controls:
	4.10.3	

ASSESSMENT PROCEDURE: MP-3.1

Assessment Objective

Determine if:

(i) the organization defines its protected environment for media labeling requirements;

(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;

(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and (iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security

markings (if any) of the information.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; information system security plan; removable storage media and information system output; other relevant documents or records.(Optional)

MP-3(CMS-1) – Enhancement (Moderate)

Control

Off-line backup storage media must be marked according to backup rotation schedule for ease of retrieval.

References: ARS: MP-3(CMS-1); IRS-1075: 4.6#1

Related Controls:

ASSESSMENT PROCEDURE: MP-3(CMS-1).1

Assessment Objective

Determine if:

Applicability: All

(i) the organization defines its protected environment for media labeling requirements;

(ii) the organization identifies media types and hardware components that are exempted from external labeling requirements;

(iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and (iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records to determine that off-line backup storage media is marked according to backup rotation schedule for ease of retrieval.

Interview: Organizational personnel with information system media protection responsibilities to determine off-line backup storage media is marked according to backup rotation schedule for ease of retrieval.

MP-4 – Media Storage (Moderate)

Control

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper, within controlled areas. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security level of the information ever recorded on it until destroyed or sanitized using CMS-approved procedures.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST SP 800-56 and 800-57 provide guidance on cryptographic key

Applicability: All	References: ARS: MP-4; FISCAM: TCC-3.2.4, TCC-3.3.1; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1; NIST 800-53/53A: MP-4; PISP: 4.10.4	Related Controls: AC-19, CP-9, CP-9(4) RA-2, SC-7
ASSESSMENT PROCEDURE: MF		
Assessment Objective		
Determine if:		
., .	led areas for information system media;	
., .	cuments the media and associated information contained on that media requiring physical protection in accordance	with an organizational assessment of risk;
	ecific measures used to protect the selected media and information contained on that media;	
	trols and securely stores information system media within controlled areas; and	
	nation system media commensurate with the FIPS 199 security categorization of the information contained on the m	edia.
Assessment Methods And Objec		turas: access control policy and procedures:
	lia protection policy; procedures addressing media storage; physical and environmental protection policy and procec nformation system media; other relevant documents or records.	dures, access control policy and procedures,
MP-4(PII-1) – Enhancement (Mod		
Control		
	nethod of cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest, consistent with NIST	SD 800 66 guidanaa
Applicability: All	References: HIPAA: 164.312(a)(2)(iv)	Related Controls: SC-13
ASSESSMENT PROCEDURE: MP		Related Controls. SC-15
	-4(F1).1	
Assessment Objective		
	approved cryptography (see SC-13, Use of Cryptography, PISP 4.16.13) to protect PII at rest.	
Assessment Methods And Objec		10
,	licenses used to protect PII at rest. Cryptography software is consistent with NIST SP 800-66 guidance and FIPS 1 determine if FIPS 140 approved cryptographic software/system for PII data at rest protection is being used.	40 approved.
MP-4(PII-2) – Enhancement (Mod		
	erale)	
Control		
	ia with other data, it should be protected as if it were entirely personally identifiable information.	Deleted Controles
	References: IRS-1075: 5.3#2.3, 5.3#3	Related Controls:
ASSESSMENT PROCEDURE: MF	-4(PII-2).1	
Assessment Objective		
a 1	ects, in its entirety, personally identifiable information when on magnetic media with other data.	
Assessment Methods And Objec		
a a	is protected to determine, in its entirety, it is controlled as Federal tax information.	
	determine if PII in its entirety is protected as personally identifiable information.	
MP-5 – Media Transport (Mod	derate)	
Control		
	nical controls shall be implemented to restrict the pickup, receipt, transfer, and delivery of media (paper and electron	ic) to authorized personnel based on the
sensitivity of the CMS information.		
Guidance	, hath diaited and in (a su dialanttee tennes years, while hand duites flack (through duites second states diaited tides di	alla) and any disital modia (a.s. sanas
Information system media includes	s both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video di v area or space for which the organization has confidence that the physical and procedural protections provided are	sks) and non-digital media (e.g., paper,
	or information system. This control also applies to portable and mobile computing and communications devices with	
	ints, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered in	
	dia (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authenticat	
employed in other information syst	ems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail s	stems that are transported outside of controll
	ent of risk guides the selection of media and associated information contained on that media requiring protection dur	
and procedures, the media requiring	ng protection during transport and the specific measures taken to protect such transported media. The rigor with whi	ch this control is applied is commensurate wi
and procedures, and media requin		

the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Applicability: All	References: ARS: MP-5; FISCAM: TAY-4.1.1, TAY-4.1.4; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.6#2, 4.6#4; NIST 800-53/53A: MP-5; PISP: 4.10.5	Related Controls: AC-19, CP-9, CP-9(4
ASSESSMENT PROCEDURE: I		-
Assessment Objective		
Determine if:		
	rsonnel authorized to transport information system media outside of controlled areas;	
	prmation system media during transport outside of controlled areas; and	
., .	activities associated with transport of information system media to authorized personnel.	
Assessment Methods And Obj		
	nedia protection policy; procedures addressing media transport; physical and environmental protection policy and proceed	
	n; list of organization-defined personnel authorized to transport information system media outside of controlled areas; info ation system audit records; other relevant documents or records.	ormation system media; information system
MP-5(1) – Enhancement (Mode		
Control		
	on digital media are protected during transport outside of controlled areas by using cryptography and tamper proof packa	aging and (a) if hand carried using secure
	e) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier.	aying and (a) it nand camed, using seculab
If the use of cryptography is not	technically feasible or the sensitive information is stored on non-digital media, written management approval (one level)	below the CIO) must be obtained prior to
transport and the information m	ust be (a) hand carried using securable container via authorized personnel, or (b) if shipped, by United States Postal Ser	rvice (USPS) Certified Mail with return rece
in tamper-proof packaging.		
Correspondence pertaining to a	single individual may be mailed through regular USPS mail, but should contain only the minimal amount of sensitive info	ormation in order to reduce the risk of
	single individual may be malled through regular oor of mail, but should contain only the minimal amount of sensitive inte	
unauthorized disclosure (e.g., p	artially masking social security numbers).	
unauthorized disclosure (e.g., p Guidance	artially masking social security numbers).	
unauthorized disclosure (e.g., p Guidance Physical and technical security	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI	PS 199 security categorization of the
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry	PS 199 security categorization of the
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity p	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used.	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry rotections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3,	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry rotections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1)	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity p Applicability: All ASSESSMENT PROCEDURE: I	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry rotections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1)	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity p Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry rotections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1)	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if:	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry rotections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity p Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled area	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects dig	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas using the organization-defined security measures.	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects dig Assessment Methods And Obj	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas using the organization-defined security measures. ects	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled areaa ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects media protection policy; procedures addressing media transport; physical and environmental protection policy and procedure	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n information system security plan	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled areaa ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects nedia protection policy; procedures addressing media transport; physical and environmental protection policy and proced r; information system media transport occurs.	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n information system security plan Interview: Organizational person	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects nedia protection policy; procedures addressing media transport; physical and environmental protection policy and procects; information system media transport ecords; other relevant documents or records. organization system media transport records; audit records; other relevant documents or records.	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu- (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n information system security plan Interview: Organizational person MP-5(2) – Enhancement (Mode	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects nedia protection policy; procedures addressing media transport; physical and environmental protection policy and procects; information system media transport ecords; other relevant documents or records. organization system media transport records; audit records; other relevant documents or records.	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu- (ii) the organization defines secu- (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n information system security plan Interview: Organizational person MP-5(2) – Enhancement (Mode Control	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry rotections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled area ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects nedia protection policy; procedures addressing media transport; physical and environmental protection policy and procects; information system media transport records; other relevant documents or records. non-el with information system media transport responsibilities.(Optional) rrate)	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu- (ii) the organization defines secu- (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n information system security plan Interview: Organizational person MP-5(2) – Enhancement (Mode Control Activities associated with the trans-	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects nedia protection policy; procedures addressing media transport; physical and environmental protection policy and procects; information system media transport ecords; other relevant documents or records. organization system media transport records; audit records; other relevant documents or records.	PS 199 security categorization of the ptographic mechanisms can provide
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu- (ii) the organization defines secu- (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n information system security plan Interview: Organizational person MP-5(2) – Enhancement (Mode Control Activities associated with the trans- Guidance	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) WP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled area ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects hedia protection policy; procedures addressing media transport; physical and environmental protection policy and procect h; information system media transport records; other relevant documents or records. ht information system media transport responsibilities.(Optional) rate)	PS 199 security categorization of the ptographic mechanisms can provide , Related Controls: s; and dures; access control policy and procedures
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I ASSESSMENT PROCEDURE: I ASSESSMENT Objective Determine if: (i) the organization defines secu- (ii) the organization defines secu- (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n information system security plan Interview: Organizational person MP-5(2) – Enhancement (Mode Control Activities associated with the tra Guidance Organizations establish docume	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 rity measures (e.g., locked container, cryptography) for information system media transported outside of controlled area ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects media protection policy; procedures addressing media transport; physical and environmental protection policy and procect r; information system media transport records; audit records; other relevant documents or records. nnel with information system media transport responsibilities.(Optional) rate) mesport of sensitive information system media are documented.	PS 199 security categorization of the ptographic mechanisms can provide , Related Controls: s; and dures; access control policy and procedures
unauthorized disclosure (e.g., p Guidance Physical and technical security information residing on the med confidentiality and/or integrity pr Applicability: All ASSESSMENT PROCEDURE: I ASSESSMENT PROCEDURE: I Assessment Objective Determine if: (i) the organization defines secu- (ii) the organization defines secu- (ii) the organization protects dig Assessment Methods And Obj Examine: Information system n information system security plan Interview: Organizational person MP-5(2) – Enhancement (Mode Control Activities associated with the trans- Guidance	artially masking social security numbers). measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FI ia, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cry otections depending upon the mechanisms used. References: ARS: MP-5(1); FISCAM: TAC-3.3; HIPAA: 164.312(c)(1); IRS-1075: 4.4#2, 4.5#2, 4.5#3, 4.6#2, 4.7.2#1, 8.2#1; NIST 800-53/53A: MP-5(1) MP-5(1).1 writy measures (e.g., locked container, cryptography) for information system media transported outside of controlled area ital and non-digital media during transport outside of controlled areas using the organization-defined security measures. ects nedia protection policy; procedures addressing media transport; physical and environmental protection policy and procect n; information system media transport records; audit records; other relevant documents or records. nel with information system media transport responsibilities.(Optional) rate) musport of sensitive information system media are documented. entation requirements for activities associated with the transport of information system media in accordance with the organization requirements for activities associated with the transport of information system media in accordance with the organization requirements for activities associated with the transport of information system media in accordance with the organization requirements for activities associated with the transport of information system media in accordance with the organization requirements for activities associated with the transport of information system media in accordance with the organization requirements for activities associated with the transport of information system media in accordance of the organization requirements for activities associated with the transport of information system media in accordance with the organization requirements for activities associated with the transport of inform	PS 199 security categorization of the ptographic mechanisms can provide , Related Controls: is; and dures; access control policy and procedures

(i) the organization defines a system of records for documenting activities associated with the transport of information system	m modia: and
(ii) the organization documents, where appropriate, activities associated with the transport of information system media usin	
Assessment Methods And Objects	
Examine: Information system media protection policy; procedures addressing media transport; physical and environmental	protection policy and procedures; access control policy and procedures;
information system security plan; information system media transport records; audit records; other relevant documents or re	
MP-5(PII-1) – Enhancement (Moderate)	
Control	
Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport sealed packing cartons while in transit.	rt of such media to authorized personnel. PII must be in locked cabinets or
Applicability: All References: IRS-1075: 4.4#1	Related Controls:
ASSESSMENT PROCEDURE: MP-5(PII-1).1	
Assessment Objective	
Determine if: (i) the organization protects and controls PII media during transport outside of controlled areas and restricts the activities as	sociated with transport of such media to authorized personnel; and
(ii) the organization uses locked cabinets or sealed packing cartons while PII data is in transit.	
Assessment Methods And Objects	
Examine: Rosters or list of authorized personnel to protect and control PII media during transit.	
Examine: Cabinets or the containers used for protecting PII during transit to determine if there is sufficient fortification to pro	otect PII.
MP-6 – Media Sanitization and Disposal (Moderate)	
Control	
 on storage devices, equipment, and hard copy documents. Media sanitization actions shall be tracked, documented, and verto ensure proper functionality. Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmer and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. and components that have processed or contained CMS information shall be followed. Inventory and disposition records for and retained. 	ntally approved manner, to facilitate the disposal of media, both electronic Approved equipment removal procedures for CMS information systems
Guidance	
Sanitization is the process used to remove information from information system media such that there is reasonable assurar information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniq public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sa Applicability: All References: ARS: MP-6; FISCAM: TAC-3.4; HIPAA: 164.310(d)(2)(i), 164	information, prevent the disclosure of organizational information to ques and procedures for media containing information deemed to be in the reuse or disposed. NIST SP 800-88 provides guidance on media antization products at http://www.nsa.gov/ia/government/mdg.cfm. 4.310(d)(2)(ii); IRS-1075: Related Controls: MA-4
4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2; NIST 800-53/53A: MP-6; PISP: 4.	10.6
ASSESSMENT PROCEDURE: MP-6.1	
Assessment Objective	
Determine if: (i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and (ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reus (iii) information system media sanitation is consistent with NIST SP 800-88.	
Assessment Methods And Objects	
Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800	0-88; media sanitization records; audit records; other relevant documents
or records.	

MP-6(0) – Enhancement (Moderate)		
Control		
I he sanitization process includes the removal of Sanitization.	all data, labels, marking, and activity records using NSA Guidance (www.nsa.gov/ia/government/mdg.cf	m) and NIST SP 800-88, Guidelines for Media
Applicability: All	References: ARS: MP-6(0); FISCAM: TAC-3.4; IRS-1075: 8.4#2, 8.4#3; NIST 800-53/53A: MP-6; PISP: 4.10.6	Related Controls:
ASSESSMENT PROCEDURE: MP-6(0).1		
Assessment Objective		
-	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ying enhancement to the baseline control.
Assessment Methods And Objects		
Examine: Information system media protection or records.	policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization reco	rds; audit records; other relevant documents
Interview: Organizational personnel with information	ation system media sanitization responsibilities.	
MP-6(CMS-1) – Enhancement (Moderate)		
Control		
	dding, hard-copy documents, using approved equipment, techniques, and procedures.	1
Applicability: All	References: ARS: MP-6(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: MP-6(CMS-1).1		
Assessment Objective		
Determine if:		
	media requiring sanitization and the appropriate sanitization techniques and procedures to be used in th	e process;
(ii) the organization sanitizes identified information (iii) information system media sanitation is consistent	on system media, both paper and digital, prior to disposal or release for reuse; and	
Assessment Methods And Objects		
•	es; other relevant documents or records to determine hard copy documents are finely shred, using a min	imum of cross-cut shredding using approved
equipment, techniques, and procedures.	s, other relevant documents of records to determine nard copy documents are intery sined, dsing a min	man of closs-cut shreading, using approved
	ation system media protection responsibilities to determine hard copy documents are finely shred, using	a minimum of cross-cut shredding, using
approved equipment, techniques, and procedure	is.	
MP-6(IRS-1) – Enhancement (Moderate)		
Control		
5 , S	nts or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destructio	n should be witnessed by an agency
employee.		
Applicability: All	References: IRS-1075: 8.4#1	Related Controls:
ASSESSMENT PROCEDURE: MP-6(IRS-1).1		
Assessment Objective		
Determine if:	en de service en entre de la destructura de la constructura de la destructura de la constructura de la constru	
., .	ency's agents or contractors during disposal unless authorized by the Internal Revenue Code; and	
(ii) the organization, generally, uses an agency e Assessment Methods And Objects	inployee to witness FTT destruction.	
	nauthorized disclose has been given to contractors or other agency agents.	
MP-CMS-1 – Media Related Records (M		
Control		
	system media shall be maintained to ensure control and accountability of CMS information. The media	related records shall contain sufficient
information to reconstruct the data in the event of		
Guidance		
	ds maintenance that a hash function (a reproducible method of turning inventory data into a (relatively) s ly so that the inventory information can be validated as not being tampered with prior to reconstructive ev	

Applicability: All	References: ARS: MP-CMS-1; FISCAM: TCC-3.2.4; HIPAA: 164.310(d)(2)(iii); IRS-1075: 3.2#3.1, 4.6#4; PISP: MP-CMS-1	Related Controls:
ASSESSMENT PROCEDURE: MP-CMS-1.1		
Assessment Objective		
Determine if the organization maintains inventory	y and disposition records for information system media to ensure control and accountability of CMS inform	mation.
Assessment Methods And Objects		
and accountability of CMS information.	es; other relevant documents or records to determine inventory and disposition records are maintained for	
control and accountability of CMS information.	ation system media protection responsibilities to determine inventory and disposition records are maintai	ned for information system media to ensure
MP-CMS-1(CMS-0) – Enhancement (Moderate	e)	
Control		
The media records must, at a minimum, contain: (a) The name of media recipient; (b) Signature of media recipient; (c) Date / time media received; (d) Media control number and contents; (e) Movement or routing information; and (f) If disposed of, the date, time, and method of c		
Applicability: All	References: ARS: MP-CMS-1(CMS-0); FISCAM: TCC-3.2.4; HIPAA: 164.310(d)(2)(iii); IRS-1075:	Related Controls:
ASSESSMENT PROCEDURE: MP-CMS-1(CM	3.2#3.1, 4.6#4	
	5-0).1	
Assessment Objective		
	and verifies media sanitization and disposal actions.	
Assessment Methods And Objects		
 and accountability of CMS information. The media (a) the name of media recipient; (b) signature of media recipient; (c) date / time media received; (d) media control number and contents; (e) movement or routing information; and (f) if disposed of, the date, time, and method of dominants 		but not limited to:
	ation system media protection responsibilities to determine inventory and disposition records are maintai The media records shall contain sufficient information to reconstruct the data in the event of a breach, inc	
(f) if disposed of, the date, time, and method of d	lestruction.	
MP-CMS-1(PII-1) – Enhancement (Moderate)		
Control		
For PII, authorized employees of the recipient m	ust be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they nust be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printo og that identifies:	

movement, and

 if disposed of, the date and r Applicability: All 	nethod of disposition. References: IRS-1075: 3.2#1	Related Controls:
ASSESSMENT PROCEDURE		Related Controls.
Assessment Objective Determine if:		
	s the securing of PII magnetic tapes/cartridges before, during, and after processing, an	ad the proper acknowledgment form is signed and returned; and
	y records maintain PII control and accountability by a log which contains:	ia the proper addression during signed and returned, and
date received		
 reel/cartridge control numbe 	r contents	
 number of records, if available 	le	
 movement, and 		
• if disposed of, the date and i		
Assessment Methods And O	•	
Examine: The PII inventory ta	ipe/cartridge log for:	
 date received reel/cartridge control numbe 	r contonto	
 number of records, if available 		
 movement, and 		
 if disposed of, the date and r 	nethod of disposition.	
MP-CMS-1(IRS-1) – Enhancei	ment (Moderate)	
Control		
For FTI, organizations are not	allowed to make further disclosures of FTI to their agents or to a contractor unless aut	thorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7)
Applicability: All	References: IRS-1075: 11.1#1	Related Controls:
ASSESSMENT PROCEDURE	: MP-CMS-1(IRS-1).1	
Assessment Objective		
Determine if the organization	allows unauthorized disclosure of FTI data to their agents or to an unauthorized contra	actor.
Assessment Methods And O	ojects	
Examine: FTI disclosure docu	umentation to determine is authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 1	11.7)
Interview: Organizational stat	ff to determine if personnel are knowledgeable of IRS Pub. 1075, sect. 11.1 and 11.7 m	egarding disclosure of FTI data.

Physical and Environmental Protection (PE) – Operational

PE-1 – Physical and Enviro	onmental Protection Policy and Procedures (Moderate)	
Control		
modification, diversion, destruction	ptection procedures shall be developed and implemented effectively to protect all CMS IT infrastructure and assets tion, loss, misuse, or theft whether accidental or intentional. These procedures shall meet all federal, state and lo s, directives, regulations, and guidelines.	
Guidance The physical and environment environmental protection polic	al protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regu can be included as part of the general information security policy for the organization. Physical and environmenta d for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and	al protection procedures can be developed for the
Applicability: All	References: ARS: PE-1; FISCAM: TSC-2.2.6, TSC-2.3.4, TSD-2.1; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1; NIST 800-53/53A: PE-1; PISP: 4.11.1	Related Controls:
ASSESSMENT PROCEDURE:	PE-1.1	
(ii) the organization dissemination(iii) responsible parties within t(iv) the organization updates p	nd documents physical and environmental protection policy and procedures; es physical and environmental protection policy and procedures to appropriate elements within the organization; ne organization periodically review physical and environmental protection policy and procedures; and nysical and environmental protection policy and procedures when organizational review indicates updates are requ	uired.
Assessment Methods And Ob		
	nmental protection policy and procedures; other relevant documents or records.	
	onnel with physical and environmental protection responsibilities.(Optional)	
ASSESSMENT PROCEDURE:	PE-1.2	
(ii) the physical and environme	ntal protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordinatior ntal protection policy is consistent with the organization's mission and functions and with applicable laws, directive ntal protection procedures address all areas identified in the physical and environmental protection policy and add	s, policies, regulations, standards, and guidance; and
Assessment Methods And Ob		
	mental protection policy and procedures; other relevant documents or records.	
	onnel with physical and environmental protection responsibilities.(Optional)	
PE-1(FIS-1) – Enhancement (I	loderate)	
Control		
	avior that may damage computer equipment is prohibited.	
Applicability: All	References: FISCAM: TSC-2.2.7	Related Controls:
ASSESSMENT PROCEDURE:	PE-1(FIS-1).1	
Assessment Objective Determine if the organization p Assessment Methods And Ok Examine: Employee behavior Examine: Employee rules of b Examine: Pertinent policies ar Interview: Information system	- ehavior. d procedures.	

PE-2 – Physical Access Authorization		
Control		in affinially designated as myblicky associated
Access lists of personnel with authorized acc	cess to facilities containing CMS information or information systems (except for those areas within the facilit Intained on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessar	les officially designated as publicly accessible
credentials (e.g. badges identification cards	s, smart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be re	y, updated. Appropriate authorization
Guidance	, smart cards) shall be issued to authorized personnel. It ersonnel who ho longer require access shall be re	
	, for example, badges, identification cards, and smart cards. The organization promptly removes from the a	and list paragonal polongar requiring ago
to the facility where the information system r		ccess list personner no longer requiring acces
Applicability: All	References: ARS: PE-2; FISCAM: TAC-2.1.1, TAC-2.1.2, TAC-2.1.4, TAC-2.2, TAC-3.1.A.3, TAC-	Related Controls:
	3.1.A.4, TAC-3.1.A.8, TSS-1.2.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	Nelated Controls.
ASSESSMENT PROCEDURE: PE-2.1		
Assessment Objective		
Determine if:		
(i) the organization identifies areas within the		
	review and approval for the physical access list and authorization credentials for the facility;	
	rent lists of personnel with authorized access to the facility where the information system resides (except fo	r those areas within the facility officially
designated as publicly accessible);		
	prization credentials (e.g., badges, identification cards, smart cards); and	
	n review and approve the access list and authorization credentials at the organization-defined frequency, a	least annually.
Assessment Methods And Objects		
Examine: Physical and environmental prote or records.	ction policy; procedures addressing physical access authorizations; authorized personnel access list; autho	rization credentials; other relevant documents
PE-2(0) – Enhancement (Moderate)		
Control		
	uthorized access to facilities containing information systems at least once every 180 days.	
Applicability: All	References: ARS: PE-2(0); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-3.1.A.4; NIST 800-53/53A: PE-2;	Related Controls:
	PISP: 4.11.2	Related Controls.
ASSESSMENT PROCEDURE: PE-2(0).1		
Assessment Objective		
Determine if the organization meets the requ	irements as specified in the baseline control and the specific CMS requirements as prescribed in this ampli	fying enhancement to the baseline control.
Assessment Methods And Objects		
Examine: Physical and environmental prote	ction policy; procedures addressing physical access authorizations; authorized personnel access list; autho	rization credentials; other relevant documents
or records.		
PE-2(PII-1) – Enhancement (Moderate)		
Control		
Create a restricted area, security room, or lo	cked room to control access to areas containing PII. These areas will be controlled accordingly.	
Applicability: All	References: IRS-1075: 4.3#1	Related Controls:
ASSESSMENT PROCEDURE: PE-2(PII-1).	1	
Assessment Objective		
Determine if:		
(i) the organization created a restricted area,	security room, or locked room to control access to areas containing PII; and	
., .	a, security room, or locked room in accordance with BPSSM.	
Assessment Methods And Objects		
Examinal Destricted grass acquirity rooms	or locked rooms that control access to areas containing PII to determine if control and fortification functions	are in accordance with RPSSM
	controlling restricted areas, security rooms, or locked rooms containing PII to determine compliance with B	

PE-3 – Physical Access Control (Moderate)

Control

Physical access control devices (e.g., keys, locks, combinations, card-readers) and/or guards shall be used to control entry to and exit from facilities containing CMS information or information systems, except for areas and/or facilities officially designated as publicly accessible. Individual access authorizations shall be verified before granting access to facilities containing CMS information or information or information systems. Physical access control devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis.

Combinations, access codes, and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry to facilities during emergency-related events shall be restricted to authorized individuals only. Access to workstations and associated peripheral computing devices shall be appropriately controlled when located in areas designated as publicly accessible.

Guidance

The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control system conforms to the requirements of FIPS 201 and NIST SP 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST SP 800-76.

Applicability: All

References: ARS: PE-3; FISCAM: TAC-3.1.A.3, TAC-3.1.A.5, TAC-3.1.A.7, TAC-3.1.A.8, TAC-3.1.B.2, TAN-2.1.1, TAN-2.1.2, TAN-2.2.1, TSD-2.1; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1; NIST 800-53/53A: PE-3; PISP: 4.11.3

Related Controls:

ASSESSMENT PROCEDURE: PE-3.1

Assessment Objective

Determine if:

(i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

(ii) the organization verifies individual access authorizations before granting access to the facility; and

(iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records. **Interview:** Organizational personnel with physical access control responsibilities.(Optional)

Test: Physical access control capability.

ASSESSMENT PROCEDURE: PE-3.2

Assessment Objective

Determine if:

(i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and

(iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records.

Test: Physical access control devices.

ASSESSMENT PROCEDURE: PE-3.3

Assessment Objective

Determine if:

(i) the access control system is consistent with FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed);

(ii) the access control system is consistent with NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and

(iii) the access control system is consistent with NIST SP 800-76 (where the token-based access control function employs biometric verification).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST SP 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records.

Test: Physical access control devices.

PE-3(CMS-1) – Enhancement (Moderate)

Control

Control data center / facility access by use of door and window locks, and security staff or physical authentication devices, such as biometrics and/or smart card / PIN combination.

Control data center / facility	ccess by use of door and window locks, and security staff	or physical authentication devices, such as bio	metrics and/or smart card / PIN combination.
Applicability: All	References: ARS: PE-3(CMS-1); IRS	S-1075: 4.6#1	Related Controls:
ASSESSMENT PROCEDUR	:: PE-3(CMS-1).1		
Assessment Objective			
Determine if the organization officially designated as pub		entry/exit points) to the facility where the information	ation system resides (except for those areas within the facility
Assessment Methods And	bjects		
data center / facility access	s controlled by use of door and window locks.		or records; other relevant documents or records to determine
	rsonnel with physical access control responsibilities to con		y use of door and window locks.
	I capability to determine data center / facility access is con	trolled by use of door and window locks.	-
PE-3(CMS-2) – Enhanceme	t (Moderate)		
Control			
•	physically secure environments, and grant access to expli		
Applicability: All	References: ARS: PE-3(CMS-2); FIS	3CAM: TAC-3.1.A.5; IRS-1075: 4.6#1	Related Controls:
ASSESSMENT PROCEDUR	.: PE-3(CMS-2).1		
Assessment Objective Determine if the organization officially designated as pub		entry/exit points) to the facility where the information	ation system resides (except for those areas within the facility
Assessment Methods And			
servers are stored and ope Interview: Organizational p Test: Physical access to Da	ted in physically secure environments protected from unau rsonnel with physical access control responsibilities to det a Center to determine servers are stored and operated in p	uthorized access. termine servers are stored and operated in phys	or records; other relevant documents or records to determine sically secure environments protected from unauthorized access unauthorized access.
PE-3(CMS-3) – Enhanceme	t (Moderate)		
Control Data centers must meet the	ninimum requirements as established by the Federal Infor	mation Systems Control Audit Manual (FISCAN	/).
Applicability: All	References: ARS: PE-3(CMS-3); FIS	SCAM: TAC-3.1.A.1, TAN-2.1.1, TAN-2.1.2; IRS	S-1075: 4.6#1 Related Controls:
ASSESSMENT PROCEDUR	: PE-3(CMS-3).1		
designated as publicly acce (ii) the organization verifies (iii) the organization also co Assessment Methods And Examine: Physical and env	sible); ndividual access authorizations before granting access to t trols access to areas officially designated as publicly acces Djects conmental protection policy; procedures addressing physic um requirements as established by the Federal Information	the facility; and ssible, as appropriate, in accordance with the or al access control; physical access control logs o	em resides (except for those areas within the facility officially rganization's assessment of risk. or records; other relevant documents or records to determine if
Control			
	acilities to authorized persons only.		

Restrict access to grounds / facilities to authorized persons only.

SSEESSMENT PROCEDURE: PE-3(CMS-4).1 Sesement Objective Determine if the organization also control saccess to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. Sesement Methods And Objects Test: Physical and environmental protection policy procedures addressing physical access control, physical access control, physical access control responsibilities to determine it access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine it access to grounds / facilities is restricted to authorized persons only. Test: Physical access control responsibilities to determine it access to grounds / facilities is restricted to authorized persons only. SSESSMENT PROCEDURE: PE-3(PII-1).1 SSESS	
Determine if the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. Seessment Methods And Objects Examine: Physical and environmental protection policy: procedures addressing physical access control, physical access control logs or records; other relevant documents or records access to grounds / facilities is restricted to authorized persons only. Interview: Organizational personnel with physical access control responsibilities to determine in access to grounds / facilities is restricted to authorized persons only. Ex3(PIL) - Enhancement (Moderate) Control PTI require two barriers to access PII under normal security: secured parimeter/locked container, tocked perimeter/secured interior, or locked perimeter/security container. PROCEDURE: PE-3(PIL).1 SeeSSMENT PROCEDURE: PE-3(PIL).1 SeeSSMENT PROCEDURE: PE-3(PIL).1 SeeSsment Objective Determine if: () the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. SeeSsment Objective Determine if: () the organization has two barriers to protect PII under normal security: SeeSsment Objective Determine if: () the organization containerizes protect PII under normal security: () the organization containerizes protect PII to determine were ther than authorized employees. Interview: Organizational personnel to determine if PI has been disclosed to unauthorized employees. Interview: Organizational personnel to determine if PI has been disclosed to unauthorized employees. Interview: Organization protect access authorization lists to secure areas. Seessment Methods And Objects Examine: Secured perimeter/locked occess authorization lists to secure areas. Seessment Methods And Objects Examine: Secured perimeter/locked access authorization lists that are for secure areas. Seessment PROCEDURE: PE-3(DIC-1).1 Seessment Objective Determine if the organ	
seesement Methods And Objects Examine: Physical and environmental protection policy: procedures addressing physical access control physical access control logs or records; other relevant documents or records access to grounds / facilities is restricted to authorized persons only. Test: Physical access control responsibilities to determine access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine the authorized employees may have access after hours. SESESSMENT PROCEDURE: PE-3(PII-1). SESESSMENT PROCEDURE: PE-3(PII	
seesement Methods And Objects Examine: Physical and environmental protection policy: procedures addressing physical access control physical access control logs or records; other relevant documents or records access to grounds / facilities is restricted to authorized persons only. Test: Physical access control responsibilities to determine access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine if access to grounds / facilities is restricted to authorized persons only. Test: Physical access control to determine the authorized employees may have access after hours. SESESSMENT PROCEDURE: PE-3(PII-1). SESESSMENT PROCEDURE: PE-3(PII	
Examine: Physical and environmental protection policy, procedures addressing physical access to grounds / facilities is restricted to authorized persons only. Interview: Organizational personnel with physical access control responsibilities to determine access to grounds / facilities is restricted to authorized persons only. E-3(PIL+1) – Enhancement (Moderate) For PII, require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protectimus be containerized in areas where other than authorized employees may have access atter hours. pplicability: All References: IRS-1075: 4.2#2 Related Controls: SSESSMENT PROCEDURE: PE-3(PIL-1).1 Ssessment Objective Determine fi of the organization containerizes protected III to determine the (2) barries are present for normal security: accured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (i) the organization containerizes protected III to determine the (2) barries are present for normal security: accured perimeter/locked container, locked perimeter/secured perimeter/security container; (ii) the organization containerizes protected III to determine the (2) barries are present for normal security: and forfification during normal hours and after duty hours. Interview: Organizational personnel to determine the fediveness of protecting PII after hours in secure containers from unauthorized personnel. Examine: Saccesta perimeter/secured contensing: SSESSMENT PROCEDURE: PE-3(DIC-1).1 Ssessment Objects Determine fi	
Interview: Organizational personnel with physical access control responsibilities to determine access to grounds / facilities is restricted to authorized persons only. #3(PIL-1) – Enhancement (Moderate) For PII, require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protect must be containerized in areas where other than authorized employees may have access after hours. SSESSMENT PROCEDURE: PE-3(PIL-1). SSESSMENT PROCEDURE: PE-3(PIL-1). SSESS	s to determine
Test: Physical access controls to determine if access to grounds / facilities is restricted to authorized perisons only. F3(PI-1) - Enhancement (Moderate) Sontrol For PIL require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. SSESSMENT PROCEDURE: PE-3(PIL-1). Issessment Objective Determine if: (i) the organization has two barriers to protect. PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (ii) the organization has two barriers to protect. PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (ii) the organization personnel to determine two (2) barriers are present for normal security. Examine: Barriers to protect PII to determine two (2) barriers are present for normal security. Examine: Cognalization personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. E43(DIR-1) - Enhancement (Moderate) Controls are estabilished to protect access authorization lists to secure areas. SSESSMENT PROCEDURE: PE-3(DIR-1).1 SSESSMENT PROCEDURE: PE-3(DIR-1).1 SSESSMENT PROCEDURE: PE-3(DIR-1).1 SSESSMENT PROCEDURE: PE-3(DIR-1).1 SSESSMENT PROCEDURE: PE-3	
Control For Pli, require two barriers to access Pli under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protectimust be containentized in areas where other than authorized employees may have access after hours. pplicability: All References: IRS-1075: 4.2#2 Related Controls: SSESSMENT PROCEDURE: PE-3(PII-1).1 Sessesment Objective Related Controls: Determine if: () the organization nas two barriers to protect Pl I under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; () the organization nas two barriers to protect Pl II of determine area where other than authorized employees may have access after hours. sessesment Methods And Objects Examine: Earriers to protect Pl II to determine the organization on personnel to determine the effectiveness of protecting Pli after hours in security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine the effectiveness of protecting Pli after hours in secure containers from unauthorized personnel. E30(0R-1) - Enhancement (Moderate) Controls are established to protect access authorization lists to secure areas such as data centers. Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 SSESSMENT Protective Discuting protect approved access authorization lists to accus authorization protects approved access authorization lists to secure areas. SSESSMENT Protective Discuting proceded coccess authorization lists to secure areas.	
For PUI, require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protect must be containerized in areas where other than authorized employees may have access after hours. Related Controls: SSESSMENT PROCEDURE: PE-3(PII-1).1 Issessment Objective Determine if. (i) the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (ii) the organization nas two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (ii) the organization secure perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine if PII to betermine if PII to beter	
must be containerized in areas where other than authorized employees may have access after hours. pplicability: All References: IRS-1075: 4.2#2 Related Controls: SSESSMENT PROCEDURE: PE-3(PII-1).1 sseessment Objective Determine if: (i) the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (ii) the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (ii) the organization has two barriers to protect PII to determine two (2) barriers are present for normal security. Examine: Barriers to protect PII to determine two (2) barriers are present for normal security. Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. Examine: Sacessenent (Moderate) Controls are established to protect access authorization lists to secure areas such as data centers. pplicability: All References: SSESSMENT PROCEDURE: PE-3(DIR-1).1 SSESSMENT PROCEDURE: PE-4:1 Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/	
must be containerized in areas where other than authorized employees may have access after hours. Related Controls: SSESSMENT PROCEDURE: PE-3(PII-1).1 Related Controls: SSESSMENT PROCEDURE: PE-3(PII-1).1 Sessement Objective Determine if: (i) the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; Ssessment Methods And Objects Examine: Barriers to protect PII to determine two (2) barriers are present for normal security. Examine: Barriers to protect PII to determine the offectiveness of protecting PII after hours in secure containers from unauthorized personnel to determine if PII has been disclosed to unauthorized employees. Interview: Organizational personnel to determine if PII has been disclosed to unauthorized employees. Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine if PII has been disclosed to unauthorized employees. Interview: Organization personel to determine if PII has been disclosed to unauthorized employees. Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 References: Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Ssessement Objective Detemine if the organization protects appr	cted information
applicability: All References: IRS-1075: 4.2#2 Related Controls: SSESSMENT PROCEDURE: PE-3(PII-1).1 ssessment Objective Determine if: 0) the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (ii) the organization has two barriers to protect PII to determine two (2) barriers are present for normal security. Examine: Sarriers to protect PII to determine two (2) barriers are present for normal security. Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine the Has been disclosed to unauthorized employees. Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Interview: Organization approaches to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Interview: Controls are established to protect access authorization lists to secure areas. Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Interview: Control for Transmission Medium (Moderate) Related Controls: Determine if the organization protects approved access authorization lists to secure areas. Interview: Cont	
Sessesment Objective Determine if: Differences: Determine if: Determine	
Sessesment Objective Determine if: Differences: Determine if: Differences: Determine if: Determine	
Determine if:	
(i) the organization has two barriers to protect PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container; (ii) the organization containerizes protected information in areas where other than authorized employees may have access after hours. Assessment Methods And Objects Examine: Barriers to protect PII to determine two (2) barriers are present for normal security. Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. E-3(DIR-1) - Enhancement (Moderate) Control Controls are established to protect access authorization lists to secure areas such as data centers. pplicability: All References: References: References: Resessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Sessessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Sessessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Sessessment Methods Short of the approved access authorization lists to secure areas. Sessessment Methods shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational accellists that carry unencrypted transmission. Protective accelerates to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect physical access to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additi	
(ii) the organization containerizes protected information in areas where other than authorized employees may have access after hours. Assessment Methods And Objects Examine: Barriers to protect PII to determine two (2) barriers are present for normal security. Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. E-C3(DR-1) – Enhancement (Moderate) Control Control Controls are established to protect access authorization lists to secure areas such as data centers. Applicability: All References: Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Sessesment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. PE-4 – Access Control for Transmission Medium (Moderate) Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system distribution and transmission lines help prevent accidential damage, disruption, and physical tampering. Additionally, physical protection applied to information system distribution and transmission lines help prevent accidential damage, disruption, and physical access to information system distribution and transmission lines help prevent accidential damage, disruption, and physical access to information system distribution and transmission lines help prevent accidential damage, disruption, and physical access to information system distribution and transmission lines help prevent accidential damage, disruption, and physical access to information system distribution and transmission lines help prevent accidential damage, disruption, and physical access to information system distribution and transmission lines help prevent accidential damag	r: and
Assessment Methods And Objects Examine: Barriers to protect PII to determine two (2) barriers are present for normal security. Examine: Secure operimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. E-3(DIR-1) - Enhancement (Moderate) Control Controls are established to protect access authorization lists to secure areas such as data centers. upplicability: All References: References: Researce models and Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Sessement Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Sessement Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Sessement Methods And Objects Examine: Protection shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organization of unencrypted information. Suidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection applicate within organization of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections applied to information system distribution of unencrypted transmissions. Protective measures to control physical tampering. Additionally, physical protection applicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: SESSMENT PROCE	,
Examine: Barriers to protect PÎI to determine two (2) barriers are present for normal security. Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. E-3(DIR-1) - Enhancement (Moderate) Control Controls are established to protect access authorization lists to secure areas such as data centers. pplicability: All References: Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Ssessment Objective Determine if the organization protects approved access authorization lists to secure areas. Ssessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Examine: Protection procedures are in place for approved access authorization lists to secure areas. Examine: Protection procedures are in place for approved access authorization lists to secure areas. Examine: Protection procedures are in place for approved access authorization lists to secure areas. Examine: Protection procedures are in place for approved access authorization lists to secure areas. Examine: Protection procedures are in place for approved access authorization lists to secure areas. Examine: Protection procedures are in place for approved access authorization lists to secure areas. Examine: Protection spelled to information system distribution and transmission lines help prevent accesdropping, in-transit modification, disruption, and/or physical tampering information. Uidiance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection applicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.1.1.4 Related Controls: SESSMENT PROCEDURE: PE-4.1	
Examine: Secured perimeter/locked containers which protect PII to determine security and fortification during normal hours and after duty hours. Interview: Organizational personnel to determine if PII has been disclosed to unauthorized employees. Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. E3(DIR-1) – Enhancement (Moderate) Control Controls are established to protect access authorization lists to secure areas such as data centers. Pplicability: All References: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Issessment Objective Determine if the organization protects approved access authorization lists that are for secure areas. Issessment Objective Determine: Protection procedures are in place for approved access authorization lists to secure areas. Issessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Ite-4 – Access Control for Transmission Medium (Moderate) iontrol Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Additionally, physical protection applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection easures to control physical access to information system distribution and transmission. Protective measures to control physical access to information system distribution and transmission. Protection easures to control physical tampering. Additionally, physical protection easures to control physical access to information system distribution and transmission. Protection easures to control physical access to information system distribution and transmission. Protection deasures to control	
Interview: Organizational personnel to determine if PII has been disclosed to unauthorized employees. Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. E3(DIR-1) – Enhancement (Moderate) Control Controls are established to protect access authorization lists to secure areas such as data centers. pplicability: All References: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Issessment Objective Determine if the organization protects approved access authorization lists that are for secure areas. Issessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Estamine: Protection procedures are in place for approved access authorization lists to secure areas. Estamine: Protection procedures are in place for approved access authorization lists to secure areas. Estamine: Protection procedures are in place for approved access authorization lists to secure areas. Estamine: Protection procedures are in place for approved access authorization lists to secure areas. Estamine: Protection procedures are in place for approved access authorization lists to secure areas. Estamine: Protection procedures are in place for approved access authorization lists to secure areas. Estamine: Protection procedures are in place for approved access authorization lists to secure areas. Estamine: Protection for Transmission Medium (Moderate) Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Suidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection ecessary to help prevent eavesdropping or in t	
Interview: Organizational personnel to determine the effectiveness of protecting PII after hours in secure containers from unauthorized personnel. F=3(DIR-1) – Enhancement (Moderate) Control Controls are established to protect access authorization lists to secure areas such as data centers. pplicability: All References: Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Sesessment Objective Determine if the organization protects approved access authorization lists that are for secure areas. Secure a	
PE-3(DIR-1) - Enhancement (Moderate) Control Controls are established to protect access authorization lists to secure areas such as data centers. upplicability: All References: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Ssessment Objective Determine if the organization protects approved access authorization lists that are for secure areas. Ssessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. PE-4 - Access Control for Transmission Medium (Moderate) Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Suidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and tins protection of cabing by conduit or cable trays. upplicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP; 4.11.4 Related Controls:	
Control Controls are established to protect access authorization lists to secure areas such as data centers. Related Controls: spplicability: All References: Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Image: Control is the organization protects approved access authorization lists that are for secure areas. Image: Control is the organization protects approved access authorization lists to secure areas. Ssessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. VE-4 - Access Control for Transmission Medium (Moderate) Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Suidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect necessary to help prevent access to information system distribution and transmission. Protection of cabling by conduct or cable trays. opplicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls:	
Controls are established to protect access authorization lists to secure areas such as data centers. Related Controls: spelicability: All References: Related Controls: SSESSMENT PROCEDURE: PE-3(DIR-1).1 Image: Control State Control State Controls: Related Controls: Ssessment Objective Determine if the organization protects approved access authorization lists that are for secure areas. Image: Control State	
Applicability: All References: Related Controls: ASSESSMENT PROCEDURE: PE-3(DIR-1).1 Image: Control State of the organization protects approved access authorization lists that are for secure areas. Image: Control State of the organization protects approved access authorization lists that are for secure areas. Assessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. PE-4 - Access Control for Transmission Medium (Moderate) Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Suidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission. Mathematical (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Applicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: ASSESSMENT PROCEDURE: PE-4.1 </td <td></td>	
SSESSMENT PROCEDURE: PE-3(DIR-1).1 Assessment Objective Determine if the organization protects approved access authorization lists that are for secure areas. Assessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. PE-4 – Access Control for Transmission Medium (Moderate) Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Suidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission ines help prevent accidental damage, disruption, and physical access to information system distribution and transmission. Protective measures to control physical access to information system distribution and transmissions. Protective measures to control physical access to information system distribution and transmission. Suidance Physical protections applied to information system distribution and transmission. Protective measures to control physical access to information system distribution and transmission. Protective measures to control physical access to information system distribution and transmission.	
Sessessment Objective Determine if the organization protects approved access authorization lists that are for secure areas. Sessessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. E-4 – Access Control for Transmission Medium (Moderate) Sontrol Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Buildance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection easures to control physical access to information system distribution and transmission. Protective measures to control physical access to information system distribution and unencrypted transmissions. Protective measures to control physical access to information system distribution and lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. pplicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls:	
Determine if the organization protects approved access authorization lists that are for secure areas. Sesessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. Sec.4 – Access Control for Transmission Medium (Moderate) Fortfol Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Fortice Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. pplicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: SESESMENT PROCEDURE: PE-4.1	
Assessment Methods And Objects Examine: Protection procedures are in place for approved access authorization lists to secure areas. PE-4 – Access Control for Transmission Medium (Moderate) Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Suidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. spplicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: ASSESSMENT PROCEDURE: PE-4.1	
Examine: Protection procedures are in place for approved access authorization lists to secure areas. PE-4 - Access Control for Transmission Medium (Moderate) Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Studance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect on help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission. Protection of cabling by conduit or cable trays. applicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: SSESSMENT PROCEDURE: PE-4.1 Control Controls:	
PE-4 – Access Control for Transmission Medium (Moderate) Sontrol Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Stuidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection sinclude: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. splicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: SSESSMENT PROCEDURE: PE-4.1 Controls: Controls:	
Control Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information. Suidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protect necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmissions. Protective measures to control physical access to information system distribution and transmissions. Protection of cabling by conduit or cable trays. pplicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: SSESSMENT PROCEDURE: PE-4.1	
Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information.	
Physical access controls shall be developed, documented, and implemented effectively to protect against eavesdropping, in-transit modification, disruption, and/or physical tampering information system transmission lines within organizational facilities that carry unencrypted information.	
information system transmission lines within organizational facilities that carry unencrypted information.	a of CMS
Guidance Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and inestination of unencrypted transmissions. Protective measures to control physical access to information system distribution and inestination of cabling by conduit or cable transmission. pplicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: SSESSMENT PROCEDURE: PE-4.1 Related Controls: Related Controls:	g - · · · · ·
Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protection accessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and ines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. pplicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: SSESSMENT PROCEDURE: PE-4.1 Controls: Controls:	
necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Applicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: ASSESSMENT PROCEDURE: PE-4.1 Controls: Controls: Controls:	ections are
Ines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Applicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: ASSESSMENT PROCEDURE: PE-4.1 SSESSMENT PROCEDURE: PE-4.1 Related Controls:	
Applicability: All References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4.11.4 Related Controls: ASSESSMENT PROCEDURE: PE-4.1 Second Secon	
SSESSMENT PROCEDURE: PE-4.1	

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams: other relevant documents or records.(Optional)

PE-4(CMS-1) – Enhancement (Moderate)

Control

Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel References: ARS: PE-4(CMS-1); FISCAM: TAC-3.2.E.1 **Related Controls:**

Applicability: All

ASSESSMENT PROCEDURE: PE-4(CMS-1).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

Interview: Organizational personnel with physical access control responsibilities to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

Test: Physical access controls to determine if access to telephone closets and information system distribution and transmission lines within organizational facilities are restricted only to authorized personnel.

PE-4(CMS-2) – Enhancement (Moderate)

Control

Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use.

Applicability: All

References: ARS: PE-4(CMS-2)

Related Controls:

ASSESSMENT PROCEDURE: PE-4(CMS-2).1

Assessment Objective

Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

Interview: Organizational personnel with physical access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

Test: Physical access controls to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.

PE-5 – Access Control for Display Medium (Moderate)

Control

Physical access controls shall be developed, documented, and implemented effectively to prevent unauthorized individuals from observing CMS sensitive information displayed on information system devices.

Guidance

It is good practice to position sensitive information display devices away from windows and areas of ingress and egress.

Applicability: All	References: ARS: PE-5; FISCAM: TAN-2.1.1; HIPAA: 164.310(b); NIST 800-53/53A: PE-5; PISP:	Related Controls:
	4.11.5	

ASSESSMENT PROCEDURE: PE-5.1

Assessment Objective

Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; other relevant documents or records.

PE-6 – Monitoring Physical Access (Moderate)

Control

Physical access to information systems shall be monitored for physical security compliance and to detect and respond to incidents. Appropriate organization officials shall periodically review physical

access records, investigate apparent security vie	plations or suspicious physical access activities, and take appropriate remedial action.	
Guidance		
	periodically and investigates apparent security violations or suspicious physical access activities. Response ability.	e to detected physical security incidents is
Applicability: All	References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN-2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6	Related Controls: IR-4
ASSESSMENT PROCEDURE: PE-6.1		
Assessment Objective		
-	access to the information system to detect and respond to physical security incidents.	
Assessment Methods And Objects		
Examine: Physical and environmental protection	n policy; procedures addressing physical access monitoring; physical access logs or records; other releva	ant documents or records.
Interview: Organizational personnel with physic		
Test: Physical access monitoring capability.		
PE-6(1) – Enhancement (Moderate)		
Control		
Monitor real-time physical intrusion alarms and s	surveillance equipment	
Applicability: All	References: ARS: PE-6(1); NIST 800-53/53A: PE-6(1)	Related Controls:
ASSESSMENT PROCEDURE: PE-6(1).1		
Assessment Objective		
Determine if the organization monitors real-time	intrusion plarme and surveillance equipment	
Assessment Methods And Objects		
	n policy; procedures addressing physical access monitoring; intrusion alarm/surveillance equipment logs	or records: other relevant decuments or
records.		or records, other relevant documents of
Interview: Organizational personnel with physic	al access monitoring responsibilities (Optional)	
PE-7 – Visitor Control (Moderate)		
Control		
	, and implemented effectively to control access to sensitive facilities and restricted / controlled areas cont	aining CMS information, information systems.
• · · ·	ted prior to being granted access to facilities or areas other than areas designated as publicly accessible.	
permanent authorization credentials are not con	sidered visitors.	
Guidance		
Government contractors and others with permar	nent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials fo	or federal employees and contractors
conform to FIPS 201, and the issuing organizati	ons for the PIV credentials are accredited in accordance with the provisions of NIST SP 800-79.	
Applicability: All	References: ARS: PE-7; FISCAM: TAC-3.1.B.3; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7;	Related Controls:
	PISP: 4.11.7	
ASSESSMENT PROCEDURE: PE-7.1		
Assessment Objective		
	access to the information system by authenticating visitors before authorizing access to the facility where the	he information system resides other than
areas designated as publicly accessible.		
Assessment Methods And Objects		
Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.		
Interview: Organizational personnel with visitor	access control responsibilities.(Optional)	
Test: Visitor access control capability.		
PE-7(1) – Enhancement (Moderate)		
Control		
Escort visitors and monitor visitor activity.		
Applicability: All	References: ARS: PE-7(1); FISCAM: TAC-3.1.B.1; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-	Related Controls:
	7(1)	
Rev 9	Page 113 of 189	BPSSM Appendix A Attachment 2

ASSESSMENT PROCEDURE: PE-7(1).1		
Assessment Objective		
Determine if the organization escorts visitors and	d monitors visitor activity, when required.	
Assessment Methods And Objects		
,	n policy; procedures addressing visitor access control; visitor access control logs or records; other releva	nt documents or records.
Interview: Organizational personnel with visitor	access control responsibilities.(Optional)	
PE-7(FIS-1) – Enhancement (Moderate)		
Control		
	el are authenticated through the use of preplanned appointments and identification checks.	
Applicability: All	References: FISCAM: TAC-3.1.B.3	Related Controls:
ASSESSMENT PROCEDURE: PE-7(FIS-1).1		
Assessment Objective		
Determine if the organization authenticates visite	ors, contractors and maintenance personnel through the use of preplanned appointments and identificati	on checks.
Assessment Methods And Objects		
Examine: Appointment and verification procedu	ires for visitors.	
Examine: Pertinent policies and procedures.		
Interview: Receptionist or security guard.		
PE-8 – Access Records (Moderate)		
Control		
	d / controlled areas that contain CMS information or information systems shall be logged. The visitor acc	cess record shall contain:
4.11.8.1. Name and organization of the person v	<i>v</i> isiting;	
4.11.8.2. Signature of the visitor;		
4.11.8.3. Form of identification;		
4.11.8.4. Date of access; 4.11.8.5. Time of entry and departure;		
4.11.8.6. Purpose of visit; and		
4.11.8.7. Name and organization of person visite	ed.	
Appropriate organization officials shall periodica	Ily review the access records, including after closeout.	
Guidance		
	for consistency and ease of use during log closeouts and the next months log generation.	
Applicability: All	References: ARS: PE-8; FISCAM: TAC-3.1.B.1, TAC-3.1.B.3; NIST 800-53/53A: PE-8; PISP: 4.11.8	Related Controls:
ASSESSMENT PROCEDURE: PE-8.1		
Assessment Objective		
Determine if:		
(i) the organization defines the frequency of revi		
	ords to the facility where the information system resides (except for those areas within the facility officially	v designated as publicly accessible) that
includes:		
 name and organization of the person visiting; signature of the visitor; 		
- form of identification;		
- date of access;		
- time of entry and departure;		
- purpose of visit;		
 name and organization of person visited and 		
	eview the visitor access logs in accordance with organization-defined frequency.	
Assessment Methods And Objects		
Examine: Physical and environmental protection	n policy; procedures addressing facility access records; information system security plan; facility access	control records; other relevant documents or
Rev. 9	Page 114 of 189	BPSSM Appendix A, Attachment 2

records.		
PE-8(0) – Enhancement (Moderate)		
Control		
	aviewed by monogoment monthly	
Visitor access records must be closed out and r Applicability: All	References: ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8	Related Controls:
	References: ARS. PE-0(0), NIST 800-53/53A. PE-0, PISP. 4.11.6	Related Controls:
ASSESSMENT PROCEDURE: PE-8(0).1		
Assessment Objective		
-	ments as specified in the baseline control and the specific CMS requirements as prescribed in	this amplifying enhancement to the baseline control.
Assessment Methods And Objects		
	on policy; procedures addressing facility access records; information system security plan (for o	organization-defined frequency for review of visitor
access records); facility access control records;		
PE-9 – Power Equipment and Power Ca	ibling (Moderate)	
Control		
Power supply control mechanisms shall be in pl	lace and supporting procedures shall be developed, documented, and implemented effectively	to maintain safe power for CMS information systems.
Guidance		
	d be included in the safe power implementation procedures. Remote backup site's power imple	
Applicability: All	References: ARS: PE-9; NIST 800-53/53A: PE-9; PISP: 4.11.9	Related Controls:
ASSESSMENT PROCEDURE: PE-9.1		
Assessment Objective		
Determine if the organization protects power eq	uipment and power cabling for the information system from damage and destruction.	
Assessment Methods And Objects		
Examine: Physical and environmental protection	on policy; procedures addressing power equipment and cabling protection; facility housing power	er equipment and cabling; other relevant documents o
records.		
PE-9(CMS-1) – Enhancement (Moderate)		
Control		
Permit only authorized maintenance personnel	to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring	g closets.
Applicability: All	References: ARS: PE-9(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: PE-9(CMS-1).	1	
Assessment Objective		
	uipment and power cabling for the information system from damage and destruction.	
Assessment Methods And Objects		
	on policy; procedures addressing power equipment and cabling protection; facility housing power	er equipment and cabling; other relevant documents o
records to determine if only authorized maintena	ance personnel are permitted to access infrastructure assets, including power generators, HVA	AC systems, cabling, and wiring closets.
	cal access control responsibilities to determine if only authorized maintenance personnel are per	ermitted to access infrastructure assets, including pow
generators, HVAC systems, cabling, and wiring	closets.	
PE-9(CMS-2) – Enhancement (Moderate)		
Control		
Power surge protection must be implemented for	or all computer equipment.	
Applicability: All	References: ARS: PE-9(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: PE-9(CMS-2).	1	
Assessment Objective		
	uipment and implements surge protection for all computers to assist in protection from damage	
Assessment Methods And Objects		e or destruction.
•		e or destruction.
Examine: Physical and environmental protection	on policy; procedures addressing power equipment and cabling protection; facility housing power	
	on policy; procedures addressing power equipment and cabling protection; facility housing power protection is implemented for all computer equipment.	
/records / diagrams to determine if power surge		er equipment and cabling; other relevant documents
/records / diagrams to determine if power surge	protection is implemented for all computer equipment.	er equipment and cabling; other relevant documents

	if power surge protection is implemented for all computer equipment.	
PE-10 – Emergency Shutoff (Moderate)		
Control		
	documented, and implemented effectively to provide the capability of shutting off threatened (e.g., due to a water leak) without endangering personnel by requiring	
Guidance		
5	n system resources may include, for example, data centers, server rooms, and ma	
Applicability: All	References: ARS: PE-10; NIST 800-53/53A: PE-10; PISP: 4.11.10	Related Controls:
ASSESSMENT PROCEDURE: PE-10.1		
Assessment Objective		
Determine if:		
	within a facility containing concentrations of information system resources (e.g., o	
	ns within a facility containing concentrations of information system resources, the t endangering personnel by requiring them to approach the equipment.	capability of shutting off power to any information system componer
Assessment Methods And Objects		
	n policy; procedures addressing power source emergency shutoff; emergency shu	toff controls or switches; other relevant documents or records.
PE-10(CMS-1) – Enhancement (Moderate)		
Control		
Implement and maintain a master power switch	or emergency cut-off switch, prominently marked and protected by a cover, for dat	ta centers, servers, and mainframe rooms.
Applicability: All	References: ARS: PE-10(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: PE-10(CMS-1).	1	
Assessment Objective		
Determine if the organization provides, for speci	fic locations within a facility containing concentrations of information system resou ened without endangering personnel by requiring them to approach the equipmen	
Assessment Methods And Objects		
determine if a master power switch or emergence Interview: Organizational personnel with physic implemented and maintained for data centers, so		d maintained for data centers, servers, and mainframe rooms. ncy cut-off switch, prominently marked and protected by a cover, is
servers, and mainframe rooms.	if a master power switch or emergency cut-off switch, prominently marked and pro	stected by a cover, is implemented and maintained for data centers
PE-11 – Emergency Power (Moderate)		
Control		
Emergency power supply control mechanisms s information system in the event of a primary pow	hall be in place and supporting procedures shall be developed, documented, and ver source loss.	implemented effectively to facilitate an orderly shutdown of the CMS
Guidance		
	hould be included in the safe power implementation procedures. The remote back he primary and backup locations will be switching to emergency power at the same the same same same same same same same sam	
Applicability: All	References: ARS: PE-11; FISCAM: TSC-2.2.5; NIST 800-53/53A: PE-11; PISP	: 4.11.11 Related Controls:
ASSESSMENT PROCEDURE: PE-11.1		
Assessment Objective		
•	rm uninterruptible power supply to facilitate an orderly shutdown of the information	n system in the event of a primary power source loss.
Assessment Methods And Objects		,
•	n policy; procedures addressing emergency power; uninterruptible power supply d	ocumentation: other relevant documents or records

PE-12 – Emergency Lighting (Moderate		
Control		
	procedures shall be developed, documented, and implemented effectively to enhance safety and availability tion and that cover emergency exits and evacuation routes shall be provided.	y. Automatic emergency lighting systems that
Guidance		
	obtain the needed information for documenting emergency lighting implementation procedures and archit	ecture.
Applicability: All	References: ARS: PE-12; NIST 800-53/53A: PE-12; PISP: 4.11.12	Related Controls:
ASSESSMENT PROCEDURE: PE-12.1		
Assessment Objective		
(ii) the organization employs and maintains autor	natic emergency lighting systems that activates in the event of a power outage or disruption; and matic emergency lighting systems that cover emergency exits and evacuation routes.	
Assessment Methods And Objects		an toot seconder a seconder suite and
evacuation routes; other relevant documents or r Test: Emergency lighting capability.	n policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighti records.	ng test records, emergency exits and
PE-13 – Fire Protection (Moderate)		
Control		
Fire protection mechanisms shall be in place and	d supporting procedures shall be developed, documented, and implemented effectively to prevent, detect d in the event of a fire shall be employed and maintained. Fire suppression and detection devices / syste ixed fire hoses, and smoke detectors.	
Guidance		
Fire suppression and detection devices/systems	include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke	e detectors.
Applicability: All	References: ARS: PE-13; FISCAM: TSC-2.2.1, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-13; PISP: 4.11.13	Related Controls:
ASSESSMENT PROCEDURE: PE-13.1		
Assessment Objective		
Determine if the organization employs and maint	ains fire suppression and detection devices/systems that can be activated in the event of a fire.	
Assessment Methods And Objects		
	n policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire supp and detection devices/systems; other relevant documents or records.	ression and detection devices/systems
PE-13(1) – Enhancement (Moderate)		
Control		
	systems that activate automatically and notify the organization and emergency responders in the event of	
Applicability: All	References: ARS: PE-13(1); NIST 800-53/53A: PE-13(1)	Related Controls:
ASSESSMENT PROCEDURE: PE-13(1).1		
Assessment Methods And Objects Examine: Physical and environmental protection	s/systems that activate automatically; and es/systems that notify the organization and emergency responders in the event of a fire. In policy; procedures addressing fire protection; facility housing the information system; alarm service leve and detection devices/systems documentation; other relevant documents or records.	el agreements; test records of fire suppression
Test: Simulated fire detection and automated no		

PE-13(2) – Enhancement (Moderate)		
Control		
	provide automatic notification of any activation to the organization and emergency responders.	
Applicability: All	References: ARS: PE-13(2); NIST 800-53/53A: PE-13(2)	Related Controls:
ASSESSMENT PROCEDURE: PE-13(2).1		
Assessment Objective		
Determine if the organization employs fire supp	ession devices/systems that provide automatic notification of any activation to the organization and en	nergency responders.
Assessment Methods And Objects	, , , , , , , , , , , , , , , , , , ,	5 7 1
	n policy; procedures addressing fire protection; fire suppression and detection devices/systems docum	entation: facility housing the information system:
alarm service level agreements; test records of	fire suppression and detection devices/systems; other relevant documents or records.	,, ,, ,, ,, ,, ,, , ,, ,
Test: Simulated activation of fire suppression d	evices/systems and automated notifications.(Optional)	
PE-13(3) – Enhancement (Moderate)		
Control		
	in facilities that are not staffed on a continuous basis.	
Applicability: All	References: ARS: PE-13(3); NIST 800-53/53A: PE-13(3)	Related Controls:
ASSESSMENT PROCEDURE: PE-13(3).1		Related Controls.
Assessment Objective		
	atic fire suppression capability in facilities that are not staffed on a continuous basis.	
Assessment Methods And Objects		
records of fire suppression and detection device	n policy; procedures addressing fire protection; facility housing the information system; alarm service le s/systems; other relevant documents or records.	evel agreements; facility staffing plans; test
Test: Simulated activation of fire suppression d	evices/systems and automated notifications.(Optional)	
PE-14 – Temperature and Humidity Cor	trols (Moderate)	
Control		
Temperature and humidity control mechanisms monitor the temperature and humidity of facilitie	shall be in place and supporting procedures shall be developed, documented, and implemented effecti s containing CMS information systems.	vely to maintain (within acceptable levels) and
Guidance		
Local building a safety codes are a good place	o obtain the needed information for documenting HVAC implementation procedures and architecture.	Consideration for Occupational Safety and
Health Administration (OSHA) requirements ma		Deleted Controles
	References: ARS: PE-14; FISCAM: TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-14; PISP: 4.11.14	Related Controls:
ASSESSMENT PROCEDURE: PE-14.1		
Assessment Objective		
Determine if:		
	cceptable levels, the temperature and humidity within the facility where the information system resides;	and
	erature and humidity within the facility where the information system resides.	
Assessment Methods And Objects		
	n policy; procedures addressing temperature and humidity control; facility housing the information syst	em; temperature and humidity controls;
	on; temperature and humidity records; other relevant documents or records.	
PE-14(CMS-1) – Enhancement (Moderate)		
Control		
Evaluate the level of alert and follow prescribed	guidelines for that alert level.	
Applicability: All	References: ARS: PE-14(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: PE-14(CMS-1)	.1	
Assessment Objective		
Determine if:		
	cceptable levels, the temperature and humidity within the facility where the information system resides;	and
Rev. 9	Page 118 of 189	RDSSM Appondix A Attachment ?
NUV. 7	1 ago 110 01 109	BPSSM Appendix A, Attachment 2

(ii) the organization regularly monitors the tempe	rature and humidity within the facility where the information system resides.	
Assessment Methods And Objects		
Examine: Physical and environmental protection	n policy; procedures addressing temperature and humidity control; facility housing the information system n; temperature and humidity records; other relevant documents or records to determine the level of aler	m; temperature and humidity controls;
	mental protection responsibilities to determine if there exists the level of alert and prescribed guidelines	
PE-14(CMS-2) – Enhancement (Moderate)		
Control		
Alert component management of possible loss o	f service and/or media	
Applicability: All	References: ARS: PE-14(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: PE-14(CMS-2).		Related Controls.
Assessment Objective	•	
	management personnel of loss of service or media.	
Assessment Methods And Objects		
-	n policy; procedures addressing temperature and humidity control; facility housing the information system	m: temperature and humidity controls:
	n; temperature and humidity records; other relevant documents or records to determine an alert is gene	
	nmental protection responsibilities to determine an alert is generated to component management of pos	sible loss of service and/or media
PE-14(CMS-3) – Enhancement (Moderate)		
Control		
Report damage and provide remedial action. Im	plement contingency plan, if necessary	
Applicability: All	References: ARS: PE-14(CMS-3)	Related Controls:
ASSESSMENT PROCEDURE: PE-14(CMS-3).		
Assessment Objective		
	the temperature and humidity within the facility where the information system resides.	
Assessment Methods And Objects		
-	n policy; procedures addressing temperature and humidity control; facility housing the information system	m; temperature and humidity controls;
	n; temperature and humidity records; other relevant documents or records to determine damage is repo	orted and remedial action is taken, including the
implementation of contingency plan.		
	nmental protection responsibilities to determine to determine if damage is reported and remedial action	is taken, including the implementation of
contingency plan.		
PE-14(FIS-1) – Enhancement (Moderate)		
Control		
Redundancy exists in the air cooling system.	References FIRCANA TOO 0.0.0	Delete d Controlo:
	References: FISCAM: TSC-2.2.3	Related Controls:
ASSESSMENT PROCEDURE: PE-14(FIS-1).1		
Assessment Objective		
Determine if the organization uses redundant air	cooling systems.	
Assessment Methods And Objects		
Examine: Entity's facilities.	A constant to the disconting systems	
Examine: Operation, location, maintenance, and Examine: Pertinent policies and procedures.	access to the all cooling systems.	
Interview: Site manager.		
PE-15 – Water Damage Protection (Mod	lerate)	
Control		
	t the building plumbing does not endanger CMS information systems. Procedures shall be developed, d	ocumented and implemented effectively to
reduce the potential damage from plumbing leak		

Cuidenee		
Guidance	a bita 'n die andere d'a fan andere andere andere andere andere andere d'an andere d'an andere andere andere b	
Health Administration (OSHA) requirements may	obtain the needed information for documenting water damage protection procedures and archited	cture. Consideration for Occupational Safety and
		Palatad Controlo
Applicability: All	References: ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15; PISP: 4.11.15	Related Controls:
ASSESSMENT PROCEDURE: PE-15.1		L.
Assessment Objective		
Determine if:		
(i) the organization identifies key personnel with	nowledge of location and operational procedures for activating master shutoff valves for plumbing	system; and
(ii) the organization protects the information syst	m from water damage resulting from broken plumbing lines or other sources of water leakage by	providing master shutoff valves that are accessible,
working properly, and known to key personnel.		
Assessment Methods And Objects		
	policy; procedures addressing water damage protection; facility housing the information system; r	
a	for master shutoff values for the plumbing system; master shutoff value documentation; other rele	vant documents or records.
Interview: Organization personnel with physical		
Test: Simulated master water shutoff value activ		
PE-16 – Delivery and Removal (Modera	e)	
Control		
	d implemented effectively to control the flow of information system-related items into and out of the	organization. Appropriate officials shall authorize
the delivery or removal of CMS information syste	m-related items.	
		controlled are containing CMC information
information systems, and media libraries.	val controls shall be implemented to isolate delivery areas from sensitive facilities and restricted /	controlled areas containing CIVIS Information,
Guidance		
	ossible, isolates the areas from the information system and media libraries to avoid unauthorized preferences: ARS: PE-16; NIST 800-53/53A; PE-16; PISP; 4.11.16	
	References: ARS: PE-16; NIS1 800-53/53A: PE-16; PISP: 4.11.16	Related Controls:
ASSESSMENT PROCEDURE: PE-16.1		
Assessment Objective		
Determine if:		
	elated items (i.e., hardware, firmware, software) entering and exiting the facility; and	
(ii) the organization maintains appropriate record	s of items entering and exiting the facility.	
Assessment Methods And Objects		
	policy; procedures addressing delivery and removal of information system components from the f	acility; facility housing the information system;
records of items entering and exiting the facility;		
	esponsibilities for information system components entering and exiting the facility.	
PE-17 – Alternate Work Site (Moderate)		
Control		
	implemented effectively to control information system security at alternate work sites. A method	of communication shall be provided to employees
at alternate work sites to report security issues o	suspected security incidents.	
Guidance		
o 1	s to communicate with information system security staff in case of security problems. NIST SP 80	0-46 provides guidance on security in
telecommuting and broadband communications.		Deleted Ocutuele
	References: ARS: PE-17; HIPAA: 164.310(a)(2)(i); NIST 800-53/53A: PE-17; PISP: 4.11.17	Related Controls:
ASSESSMENT PROCEDURE: PE-17.1		
Assessment Objective		
Determine if the organization employs appropria	e management, operational, and technical information system security controls at alternate work s	ites.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records.

Interview: Organization personnel using alternate work sites.

PE-17(CMS-1) – Enhancement (Moderate)

Control

Employ appropriate security controls at alternate work sites. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

Applicability: All	References: ARS: PE-17(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: PE-17(CMS-1)	1	

Assessment Objective

Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records to determine if appropriate security controls at alternate work sites are employed. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

Interview: Organizational personnel with alternate worksite responsibilities to determine if appropriate security controls at alternate work sites are employed. Security controls may include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems when not in use.

PE-18 – Location of Information System Components (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that information system components are positioned within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.

Guidance

Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Applicability: All	References: ARS: PE-18; FISCAM: TAN-2.1.1, TAN-2.1.2; HIPAA: 164.312(c)(1); NIST 800-53/53A: PE-18; PISP: 4.11.18	Related Controls:
ASSESSMENT PROCEDURE: PE-18.1		

ASSESSMENT PROCEDURE: PE-18.1

Assessment Objective

Determine if:

(i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and

(ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; other relevant documents or records.

Planning (PL) – Management

PL-1 – Security Planning Policy and Procedures (Moderate)

Control

All CMS information systems and major applications shall be documented in a SSP, which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, in accordance with current CMS Procedures.

Guidance

The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-18 provides guidance on security planning. NIST SP 800-12 provides guidance on security policies and procedures.

References: ARS: PL-1; FISCAM: TSP-2.1, TSP-3.2; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2; NIST 800-53/53A: PL-1; PISP: 4.12.1	Related Controls:

ASSESSMENT PROCEDURE: PL-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security planning policy and procedures;

(ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review security planning policy and procedures; and

(iv) the organization updates security planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: PL-1.2

Assessment Objective

Determine if:

(i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

References: FISCAM: TSP-3.3.2

PL-1(FIS-1) – Enhancement (Moderate)

Control

Security policies are distributed to all affected personnel.

Applicability: All

ASSESSMENT PROCEDURE: PL-1(FIS-1).1

Assessment Objective

Determine if the organization distributes security policies to all affected personnel.

Assessment Methods And Objects

Examine: Memos, electronic mail files, or other policy distribution mechanisms.

Interview: Staff and system users to determine how security policies are distributed.

PL-2 – System Security Plan (SSP) (Moderate)

Control

All CMS information systems and major applications shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18. The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization

Related Controls:

	ources management strategic plan. The information contained in the SSP is subject to reporting require s, standards, and guidance, including, but not limited to, current CMS Procedures.	ments as established by applicable laws,	
Guidance			
The security plan is aligned with the organization	's information system architecture and information security architecture. NIST SP 800-18 provides guida	nce on security planning.	
Applicability: All	References: ARS: PL-2; FISCAM: TAC-3.1.A.1, TSP-2.1, TSP-3.2; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3; NIST 800-53/53A: PL-2; PISP: 4.12.2	Related Controls:	
ASSESSMENT PROCEDURE: PL-2.1			
Assessment Objective			
 (iii) the security plan development is consistent w and supplementation of the tailored baseline; (iv) the security plan is consistent with the organi (v) designated organizational officials review and Assessment Methods And Objects Examine: Security planning policy; procedures a relevant documents or records. 	security requirements for the information system and a description of the security controls planned or in with NIST SP 800-18 and the concepts in the NIST Risk Management Framework including baseline securitation's information system architecture and information security architecture; and approve the security plan.	urity control selection, tailoring of the baseline,	
	ation system security planning and plan implementation responsibilities.		
PL-2(CMS-1) – Enhancement (Moderate)			
Control	atom according to the CMC System Convrity Plan (SSD) Bracedures		
Applicability: All	stem according to the CMS System Security Plan (SSP) Procedures. References: ARS: PL-2(CMS-1); FISCAM: TSP-2.1; HIPAA: 164.316(b)(1)(ii), 164.316(b)(1)(ii); HSPD	Related Controls:	
	7: J(35); IRS-1075: 4.7.3#2	Related Controls.	
ASSESSMENT PROCEDURE: PL-2(CMS-1).1			
Assessment Objective			
Determine if: (i) the organization develops and implements a security plan for the information system; (ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements; (iii) the security plan is consistent with NIST SP 800-18; (iv) the security plan is consistent with the organization's information system architecture and information security architecture; and (v) designated organizational officials review and approve the security plan. Assessment Methods And Objects Examine: Security planning policy; procedures addressing information system security plan development and implementation; NIST SP 800-18; security plan for the information system; other relevant documents or records to determine the in-place security controls of the system are documented according to the CMS System Security Plan (SSP) Procedures. Interview: Organizational personnel with information system security planning and plan implementation responsibilities to determine if System Security Plan (SSP) includes the in-place security controls of the system and are documented according to the CMS System Security Plan (SSP) Procedures.			
PL-2(PII-1) – Enhancement (Moderate)			
Control			
•	responsible for implementing the procedures to which the documentation pertains.		
	References: HIPAA: 164.316(b)(2)(ii)	Related Controls:	
ASSESSMENT PROCEDURE: PL-2(PII-1).1			
Assessment Objective Determine if the organization provides to those persons responsible for implementing the procedures to which the documentation pertains. Assessment Methods And Objects Examine: Procedures that document who obtains documentation and which documentation pertains to whom for implementation. Interview: Organizational personnel who are responsible for implementation of procedures to determine if documentation is available.			
D 0	Dec. 122 - 6190		

PL-2(HIP-1) – Enhancement (M	oderate)	
Control		
Retain documentation of policie	s and procedures relating to HIPAA 164.306 for 6 years from the date of its creation c	or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)
Applicability: All	References: HIPAA: 164.316(b)(2)(i)	Related Controls:
ASSESSMENT PROCEDURE:	PL-2(HIP-1).1	
Assessment Objective		
	tains documentation of policies and procedures relating to 164.306 for six (6) years fr	rom the date of its creation or the date when it last was in effect, whichever is later
Assessment Methods And Ob	ects	
Examine: A sampling of docum (See HIPAA 164.316(b))	entation of policies and procedures relating to 164.306 is held for six (6) years from the	he date of its creation or the date when it last was in effect, whichever is later.
Interview: Organization person effect, whichever is later. (See I	nel to determine if documentation of policies and procedures relating to 164.306 is he HIPAA 164.316(b))	eld for six (6) years from the date of its creation or the date when it last was in
PL-2(IRS-1) – Enhancement (M	oderate)	
Control		
When FTI is incorporated into a	Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed	ed, in addition to those specified in other controls.
Applicability: All	References: IRS-1075: 5.6.3.5#3	Related Controls:
ASSESSMENT PROCEDURE:	PL-2(IRS-1).1	
Assessment Objective		
	corporates FTI into a Data Warehouse, the controls described in IRS Pub. 1075, Exhi	ibit 7 are to be followed, in addition to those specified in other controls.
Assessment Methods And Obj		
-	e compliance with IRS Pub 1075 Exhibit 7 while FTI is incorporated into a Data Wareh	house
PL-2(IRS-2) – Enhancement (M		
from the IRS. Annually thereaft also advises the IRS of future a that the organization is protectir	Safeguard Procedures Report (SPR) that describes the procedures established and u er, the organization must file a Safeguard Activity Report (SAR). The SAR advises the ctions that will affect the organization's safeguard procedures, summarizes the organi ng FTI pursuant to IRC Section 6103(p)(4) and the organization's own security require	e IRS of minor changes to the procedures or safeguards described in the SPR. It ization's current efforts to ensure the confidentiality of FTI, and finally, certifies
	I. (See IRS Pub. 1075, sections 7 & 8)	
Applicability: All	References: IRS-1075: 7.1#1, 7.1#2, 7.1#3, 8.1#1	Related Controls:
ASSESSMENT PROCEDURE:	PL-2(IRS-2).1	
Assessment Objective		
the information received from th described in the SPR. It also ad FTI, and finally, certifies that the	evelops and submits a Safeguard Procedures Report (SPR) that describes the procedure IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SA livises the IRS of future actions that will affect the organization's safeguard procedures organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization I be updated and resubmitted. (See IRS Pub. 1075, sections 7 & 8).	AR). The SAR advises the IRS of minor changes to the procedures or safeguards s, summarizes the organization's current efforts to ensure the confidentiality of
Examine: Safeguard Procedure	e Reports to determine the procedures established and used ensure confidentially of t	the FTI data received from the IRS.
	eports to determine annual submission and protections are in accordance with the Sa	
PL-3 – System Security Pla		
Control		
The SSP shall be reviewed at le	east every 365 days and updated minimally every three (3) years to reflect current cor tions that may impact security; when the data sensitivity level increases; after a serior	
Guidance		
Significant changes are defined	in advance by the organization and identified in the configuration management proce	ess. NIST SP 800-18 provides guidance on security plan updates.
Rev. 9	Page 124 of 189	BPSSM Appendix A, Attachment
	1 460 121 01 109	Di boin Appendix A, Attachinen

Applicability: All References: ARS: PL-3; FISCAM: TSP-2.2; HIPAA: 164.306(a)(3), 164.316(a), 164.316(b)(2)(iii); Related Controls: HSPD 7: G(24), J(35): IRS-1075: 5.6.1.2#1.4: NIST 800-53/53A: PL-3: PISP: 4.12.3 **ASSESSMENT PROCEDURE: PL-3.1** Assessment Objective Determine if: (i) the organization defines the frequency of information system security plan reviews and updates; (ii) the organization updates the security plan in accordance with organization-defined frequency, at least annually; (iii) the organization receives input to update the security plan from the organization's configuration management and control process; and (iv) the updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls. **Assessment Methods And Objects** Examine: Security planning policy; procedures addressing information system security plan updates; information system security plan; configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records. PL-4 – Rules of Behavior (ROB) (Moderate) Control ROBs shall be established, and made readily available, to delineate clearly user responsibilities and expected behavior of all Business Owners, users, operators, and administrators with regard to information and information system usage. Before authorizing access to the information system and / or information and annually thereafter, the organization shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the ROBs. Specific ROBs shall be established to govern work-at-home users who access CMS information or information systems. Limited personal use of organization-owned or leased equipment and resources shall be considered to be a permitted use of organization-owned or leased equipment and resources when the following conditions are met: 4.12.4.1. Such use involves minimal additional expense to CMS: 4.12.4.2. Such use does not interfere with the mission or operation of CMS; 4.12.4.3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch; 4.12.4.4. Such use does not overburden any CMS information system resources: 4.12.4.5. Such use is not otherwise prohibited under this policy; and 4.12.4.6. Any use of organizational Internet and email resources shall be made with the understanding that such use is not secure, private or anonymous. The following uses of organization-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited: 4.12.4.7. Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace; 4.12.4.8. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords; 4.12.4.9. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity; 4.12.4.10. All email communications to groups of employees that are subject to approval prior to distribution and have not been approved by the organization (e.g., retirement announcements, union notices or announcements, charitable solicitations); and 4.12.4.11. Employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees. All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of organization-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that employees desire to protect their privacy, employees shall not use organization-owned or leased equipment and resources. Guidance Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST SP 800-18 provides guidance on preparing rules of behavior. Applicability: All References: ARS: PL-4; FISCAM: TSP-3.3.2; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: **Related Controls:** 5.6.1.2#1.5; NIST 800-53/53A: PL-4; PISP: 4.12.4 ASSESSMENT PROCEDURE: PL-4.1 Assessment Objective Determine if: (i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage; (ii) the organization makes the rules available to all information system users;

(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and

(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.			
Assessment Methods And Objects			
•	addressing rules of behavior for information system users; NIST SP 800-18; rules of behav	vior: other relevant documents or records	
	thorized users of the information system and have signed rules of behavior.	nor, other relevant documents of records.	
PL-4(CMS-1) – Enhancement (Moderate)			
Control			
Define user roles and expectations for system an Applicability: All	References: ARS: PL-4(CMS-1)	Related Controls:	
ASSESSMENT PROCEDURE: PL-4(CMS-1).1		Related Controls.	
Assessment Objective			
Determine if:			
	t describe user responsibilities and expected behavior with regard to information system us	sage:	
(ii) the organization makes the rules available to			
(iii) the rules of behavior for organizational perso	· · · · ·		
(iv) the organization receives a signed acknowle	dgement from users indicating that they have read, understand, and agree to abide by the	rules of behavior, before authorizing access to the	
information system and its resident information.		-	
Assessment Methods And Objects			
Examine: Security planning policy; procedures f	for the development and implementation of rules of behavior for information system users;	NIST SP 800-18; rules of behavior; other relevant	
	nd expectations for system and network use are defined.		
o 1	thorized users of the information system and have signed rules of behavior to determine u	ser roles and expectations for system and network use are	
defined.			
PL-4(CMS-2) – Enhancement (Moderate)			
Control			
Electronic signatures are acceptable as signed a	acknowledgement of rules-of-behavior (ROB).		
	9		
Applicability: All	References: ARS: PL-4(CMS-2)	Related Controls:	
	References: ARS: PL-4(CMS-2)	Related Controls:	
Applicability: All	References: ARS: PL-4(CMS-2)	Related Controls:	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1	References: ARS: PL-4(CMS-2)	Related Controls:	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system use		
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users;		
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational person	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and	sage;	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational person	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users;	sage;	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational perso (iv) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and dgement from users indicating that they have read, understand, and agree to abide by the	sage; rules of behavior, before authorizing access to the	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational perso (iv) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and degement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users;	sage; rules of behavior, before authorizing access to the	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational perso (iv) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic signed	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and edgement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB).	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational persoc (iv) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic sig Interview: Organizational personnel who are au	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and degement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users;	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational perso (iv) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic sig Interview: Organizational personnel who are au acknowledgement of rules-of-behavior (ROB).	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and degement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). thorized users of the information system and have signed rules of behavior to determine e	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational perso (iv) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic sig Interview: Organizational personnel who are au	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and degement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). thorized users of the information system and have signed rules of behavior to determine e	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the organization makes the rules available to (iii) the rules of behavior for organizational persoc (iv) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic signed Interview: Organizational personnel who are au acknowledgement of rules-of-behavior (ROB). PL-5 – Privacy Impact Assessment (PIA Control	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and edgement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). thorized users of the information system and have signed rules of behavior to determine e) (Moderate)	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant lectronic signatures are acceptable as signed	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic signed acknowledgement of rules-of-behavior (ROB). PL-5 – Privacy Impact Assessment (PIA Control	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and adgement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). thorized users of the information system and have signed rules of behavior to determine e) (Moderate) stems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandu	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant lectronic signatures are acceptable as signed	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic signet acknowledgement of rules-of-behavior (ROB). PL-5 – Privacy Impact Assessment (PIA Control PIAs shall be conducted for CMS information system	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and adgement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). thorized users of the information system and have signed rules of behavior to determine e) (Moderate) stems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandu	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant lectronic signatures are acceptable as signed	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the organization makes the rules available to (iii) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic sig Interview: Organizational personnel who are au acknowledgement of rules-of-behavior (ROB). PL-5 – Privacy Impact Assessment (PIA Control PIAs shall be conducted for CMS information system Guidance	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and adgement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). thorized users of the information system and have signed rules of behavior to determine e) (Moderate) stems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandu	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant lectronic signatures are acceptable as signed	
Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the rules of behavior for organizational perso (iv) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic sig Interview: Organizational personnel who are au acknowledgement of rules-of-behavior (ROB). PL-5 – Privacy Impact Assessment (PIA Control PIAs shall be conducted for CMS information system and regulations Guidance OMB Memorandum 03-22 provides guidance for	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and adgement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). ithorized users of the information system and have signed rules of behavior to determine e) (Moderate) stems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandus.	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant lectronic signatures are acceptable as signed	
 Applicability: All ASSESSMENT PROCEDURE: PL-4(CMS-2).1 Assessment Objective Determine if: (i) the organization establishes a set of rules tha (ii) the organization makes the rules available to (iii) the organization makes the rules available to (iii) the organization receives a signed acknowle information system and its resident information. Assessment Methods And Objects Examine: Security planning policy; procedures f documents or records to determine electronic significational personnel who are au acknowledgement of rules-of-behavior (ROB). PL-5 – Privacy Impact Assessment (PIA Control PIAs shall be conducted for CMS information synAccountability Act (HIPAA) rules and regulations Guidance OMB Memorandum 03-22 provides guidance for 	References: ARS: PL-4(CMS-2) t describe user responsibilities and expected behavior with regard to information system us all information system users; onnel are consistent with NIST SP 800-18; and edgement from users indicating that they have read, understand, and agree to abide by the for the development and implementation of rules of behavior for information system users; gnatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). thorized users of the information system and have signed rules of behavior to determine e (Moderate) stems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandus. r implementing the privacy provisions of the E-Government Act of 2002.	sage; rules of behavior, before authorizing access to the NIST SP 800-18; rules of behavior; other relevant lectronic signatures are acceptable as signed um M-03-22, and the Health Insurance Portability and	

			1
SS, ZPIC			
ASSESSMENT PROCEDURE: PL-5.1			
Assessment Objective			
Determine if:			
	assessment on the information system in accordance with OMB policy; and		
(ii) the privacy impact assessment is consisten	t with federal legislation and OMB policy.		
Assessment Methods And Objects			
Examine: Security planning policy; procedures relevant documents or records.	addressing privacy impact assessments on the information system; appropriate f	federal legislation and Ol	MB policy; privacy impact assessment; other
PL-6 – Security-Related Activity Planni	ng (Moderate)		
Control			
Security-related activities affecting the information	ion system shall be planned and coordinated before being performed in order to r	educe the impact on CM	IS operations (i.e., mission, functions, image,
	viduals. Routine security-related activities include, but are not limited to, security		
security certifications, and testing / exercises.	Organizational advance planning and coordination includes both emergency and	non-emergency (i.e., rou	itine) situations.
Guidance			
	are not limited to, security assessments, audits, system hardware and software ma	aintenance, security certi	ifications, and testing/exercises.
	tion includes both emergency and non-emergency (i.e., routine) situations.		
Applicability: All	References: ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6		Related Controls:
ASSESSMENT PROCEDURE: PL-6.1			
Assessment Objective			
Determine if:			
	rity-related activities affecting the information system before conducting such activities	vities in order to reduce t	the impact on organizational operations,
5	organizational assets, and individuals; and		
	ordination of security-related activities includes both emergency and non-emerger	ncy situations.	
Assessment Methods And Objects			
	addressing security-related activity planning for the information system; other rel	evant documents or reco	oras.
Interview: Organizational personnel with inform	nation system security planning and plan implementation responsibilities.		

Personnel Security (PS) - Operational

PS-1 – Personnel Security Policy and	Brocoduros (Moderato)	
	Procedures (moderate)	
Control	and an units controls consistent with an elicable laws. Even time Orders, as listen, dispetiture, resultations, a	andarda, and avidalizas. Dressduras shall be
	nnel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations, s	andards, and guidelines. Procedures shall be
developed to guide the implementation of pers	solinei security controls.	
Guidance		
I he personnel security policy and procedures	are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and gu curity policy for the organization. Personnel security procedures can be developed for the security program	dance. The personnel security policy can be
	ides guidance on security policies and procedures.	i in general, and for a particular information
Applicability: All	References: ARS: PS-1; FISCAM: TSD-1.3.3; IRS-1075: 5.6.2.1#1.1-2; NIST 800-53/53A: PS-1;	Related Controls:
	PISP: 4.13.1	Related Controls.
ASSESSMENT PROCEDURE: PS-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and documents	personnel security policy and procedures;	
	ecurity policy and procedures to appropriate elements within the organization;	
(iii) responsible parties within the organization	periodically review personnel security policy and procedures; and	
	ity policy and procedures when organizational review indicates updates are required.	
Assessment Methods And Objects		
Examine: Personnel security policy and proce	edures, other relevant documents or records.	
Interview: Organizational personnel with pers	sonnel security responsibilities.(Optional)	
ASSESSMENT PROCEDURE: PS-1.2		
Assessment Objective		
Determine if:		
	rpose, scope, roles and responsibilities, management commitment, coordination among organizational en	ities, and compliance;
(ii) the personnel security policy is consistent	with the organization's mission and functions and with applicable laws, directives, policies, regulations, sta	ndards, and guidance; and
(iii) the personnel security procedures address	s all areas identified in the personnel security policy and address achieving policy-compliant implementation	ns of all associated security controls.
Assessment Methods And Objects		
Examine: Personnel security policy and proce	edures; other relevant documents or records.	
Interview: Organizational personnel with personnel		
PS-1(FIS-1) – Enhancement (Moderate)		
Control		
	c basis and controlled to ensure that objectives laid out in job descriptions are carried out.	
Applicability: All	References: FISCAM: TSD-2.2.1	Related Controls:
ASSESSMENT PROCEDURE: PS-1(FIS-1).		
Assassment Objective		
		rrind out
Determine if the organization monitors staff pe	erformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are ca	rried out.
Determine if the organization monitors staff per Assessment Methods And Objects		rried out.
Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures.	erformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are ca	
Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions required	erformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are ca ing supervisory review and approval for evidence of such performance (e.g., approval of input of transaction	
Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions require Interview: Management and subordinate personal sub	erformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are ca ing supervisory review and approval for evidence of such performance (e.g., approval of input of transaction	
Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions require Interview: Management and subordinate person PS-1(FIS-2) – Enhancement (Moderate)	erformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are ca ing supervisory review and approval for evidence of such performance (e.g., approval of input of transaction	
Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions requir Interview: Management and subordinate pers PS-1(FIS-2) – Enhancement (Moderate) Control	erformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are ca ing supervisory review and approval for evidence of such performance (e.g., approval of input of transactions sonnel.	ons, software changes).
Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions require Interview: Management and subordinate person PS-1(FIS-2) – Enhancement (Moderate) Control	erformance on a periodic basis and is controlled to ensure that objectives laid out in job descriptions are ca ing supervisory review and approval for evidence of such performance (e.g., approval of input of transaction	ons, software changes).

ASSESSMENT PROCEDURE: PS-1(FIS-2).1

Assessment Objective

Determine if the organization regularly schedules vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.

Assessment Methods And Objects

Examine: Personnel records to identify individuals who have not taken vacation or sick leave in the past year.

Examine: Staff assignment records and determine whether job and shift rotations occur.

Examine: Vacation and job rotation policies and procedures.

Interview: Information system management and users.

PS-1(FIS-3) – Enhancement (Moderate)

Control

Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes. Employees are made aware of their job descriptions.

Applicability: All	References: FISCAM: TSD-1.2.2, TSD-1.3.1, TSP-4.2.1, TSS-2.1.2, TSS-2.1.3	Related Controls:

ASSESSMENT PROCEDURE: PS-1(FIS-3).1

Assessment Objective

Determine if:

(i) the organizational documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes.

(ii) the organization makes the employees aware of their job descriptions.

Assessment Methods And Objects

Examine: Effective dates of the position descriptions and determine whether they are current.

Examine: Job descriptions for several positions in organizational units and for user security administrators.

Examine: Job descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.

Interview: Management personnel.

PS-2 – Position Categorization (Moderate)

Control

A criticality / sensitivity rating (e.g., non-sensitive, national security, public trust) shall be assigned to all positions within the organization. The criticality / sensitivity rating shall be in compliance with 5 CFR 731.106(a), Executive Orders 10450 and 12968, NSPD-1, HSPD-7, and HSPD-12 and consistent with OPM policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating. All criticality / sensitivity ratings must be submitted to the DHHS HR department and CMS' personnel security department.

Guidance

Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Applicability: All	References: ARS: PS-2; IRS-1075: 5.6.2.1#1.3; NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:
ASSESSMENT DRACEDURE, DS 24		

ASSESSMENT PROCEDURE: PS-2.1

Assessment Objective

Determine if:

(i) the organization assigns a risk designations to all positions within the organization;

(ii) the organization establishes a screening criteria for individuals filling organizational positions;

(iii) the risk designations for the organizational positions are consistent with applicable federal regulations and OPM policy and guidance;

(iv) the organization defines the frequency of risk designation reviews and updates for organizational positions; and

(v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan; records of risk designation reviews and updates; other relevant documents or records.

PS-2(0) – Enhancement (Moderate)

Control

Review and revise position risk designations every 365 days.

Applicability: All	References: ARS: PS-2(0); NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:
ASSESSMENT PROCEDURE: PS-2(0).1		
Assessment Objective		
Determine if the organization meets the requirer	nents as specified in the baseline control and the specific CMS requirements as prescribed in this ampl	fying enhancement to the baseline control.
ssessment Methods And Objects		
	addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance	
	organization-defined frequency for review of position categorizations); records of risk designation review	s and updates; other relevant documents or
records.		
PS-3 – Personnel Screening (Moderate		
Control		
	d contractors who require access to CMS information or information systems shall be screened and reir	
	prospective employees, references background checks shall be performed before issuance of a User ID	. Security agreements shall be required for
employees and contractors assigned to work with	in mission critical information.	
Suidance	(ii) Office of Descended Management relies, resulting and widered (iii) experientical relies, result	tions, and middeness (iv) FIPC 201 and CP 20
	(ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regula blished for the risk designation of the assigned position.	tions, and guidance; (IV) FIPS 201 and SP 80
Applicability: All	References: ARS: PS-3; FISCAM: TSP-4.1.1, TSP-4.1.2; IRS-1075: 5.6.2.1#1.4; NIST 800-53/53A:	Related Controls:
	PS-3; PISP: 4.13.3	
SSESSMENT PROCEDURE: PS-3.1		
Assessment Objective		
Determine if:		
	access to organizational information and information systems prior to authorizing access; and	
	propriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73, 800-76, a	ad 800.78, and the criteria established for the
risk designation for the assigned position.		
Assessment Methods And Objects		
	addressing personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76,	and 800-78: other relevant documents or
records.	3,,	
PS-3(0) – Enhancement (Moderate)		
Control		
Perform criminal history check for all persons pr	ior to employment.	
Applicability: All	References: ARS: PS-3(0); FISCAM: TSP-4.1.2; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:
SSESSMENT PROCEDURE: PS-3(0).1		+
Assessment Objective		
	nents as specified in the baseline control and the specific CMS requirements as prescribed in this ampli	fving enhancement to the baseline control
Assessment Methods And Objects		
•	for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-76, and 800-	78: other relevant decuments or records
S-30 MS-1) - Enhancement (Moderate)		ro, other relevant documents of records.
		ro, other relevant documents of records.
Control		
control Require personnel to obtain and hold a moderat	e-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook.	
ontrol Require personnel to obtain and hold a moderat pplicability: All	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:
Control Require personnel to obtain and hold a moderat pplicability: All SSESSMENT PROCEDURE: PS-3(CMS-1).1	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	
Control Require personnel to obtain and hold a moderat Applicability: All ASSESSMENT PROCEDURE: PS-3(CMS-1).1	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	
Control Require personnel to obtain and hold a moderat Applicability: All ASSESSMENT PROCEDURE: PS-3(CMS-1).1 Assessment Objective Determine if:	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	
Control Require personnel to obtain and hold a moderat Applicability: All ASSESSMENT PROCEDURE: PS-3(CMS-1).1 Assessment Objective Determine if: (i) the organization screens individuals requiring	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:
Control Require personnel to obtain and hold a moderat Applicability: All ASSESSMENT PROCEDURE: PS-3(CMS-1).1 Assessment Objective Determine if: (i) the organization screens individuals requiring (ii) the personnel screening is consistent with ap	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:
Control Require personnel to obtain and hold a moderat Applicability: All ASSESSMENT PROCEDURE: PS-3(CMS-1).1 Assessment Objective Determine if: (i) the organization screens individuals requiring	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:
Applicability: All ASSESSMENT PROCEDURE: PS-3(CMS-1).1 Assessment Objective Determine if: (i) the organization screens individuals requiring (ii) the personnel screening is consistent with ap	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; and other relevant documents or records to determine that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

Interview: Personnel with personnel screening responsibilities to confirm that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

PS-4 – Personnel Termination (Moderate)

Control

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information and information systems is removed upon personnel termination. Termination procedures shall address:

4.13.4.1. Exit interviews;

4.13.4.2. Retrieval of all organizational information system-related property;

4.13.4.3. Notification to security management;

4.13.4.4. Revocation of all system access privileges;

4.13.4.5. Immediately escorting employees terminated for cause out of organization facilities; and

4.13.4.6. Hard disk back up and sanitization before re-issuance.

Appropriate personnel shall have access to official records created by the terminated employee that are stored on organizational information systems.

Guidance

Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Applicability: All	References: ARS: PS-4; FISCAM: TAC-2.1.6, TSP-4.1.6; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075:	Related Controls:
	5.6.2.1#1.5; NIST 800-53/53A: PS-4; PISP: 4.13.4	

ASSESSMENT PROCEDURE: PS-4.1

Assessment Objective

Determine if:

(i) the organization terminates information system access upon termination of individual employment;

(ii) the organization conducts exit interviews of terminated personnel;

(iii) the organization retrieves all organizational information system-related property from terminated personnel; and

(iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.

PS-4(CMS-1) – Enhancement (Moderate)

Control

Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

Applicability: All	References: ARS: PS-4(CMS-1); FISCAM: TAC-3.2.C.4	Related Controls:
ASSESSMENT PROCEDURE: PS-4(CMS-1).1		

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process. Interview: Personnel with termination responsibilities to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process.

PS-5 – Personnel Transfer (Moderate)

Control

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information or information systems no longer required in the new assignment is

terminated upon personnel transfer. Transfer procedures shall address:

4.13.5.1. Re-issuing appropriate organizational information system-related property (e.g., keys, identification cards, building passes);

4.13.5.2. Notification to security management;

4.13.5.3. Closing obsolete accounts and establishing new accounts: and

4.13.5.4. Revocation of all system access privileges (if applicable).

Guidance

Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts.

Applicability: All	References: ARS: PS-5; FISCAM: TAC-2.1.6, TSP-4.1.6; IRS-1075: 5.6.2.1#1.6; NIST 800-53/53A: PS-5; PISP: 4.13.5	Related Controls:
ASSESSMENT PROCEDURE: PS-5.1		

Assessment Objective

Determine if:

(i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and

(ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

PS-6 – Access Agreements (Moderate)

Control

Individuals who require access to CMS information or information systems shall be required to complete and sign appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements.

Guidance

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Applicability: All	References: ARS: PS-6; FISCAM: TSP-4.1.3; IRS-1075: 5.6.2.1#1.7; NIST 800-53/53A: PS-6; PISP: 4.13.6	Related Controls:
AGGEGGMENT PROGEDURE DO 64		

ASSESSMENT PROCEDURE: PS-6.1

Assessment Objective

Determine if:

(i) the organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access;

(ii) organizational personnel sign access agreements;

(iii) the organization defines the frequency of reviews and updates for access agreements; and

(iv) the organization reviews and updates the access agreements in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan; access agreements; records of access agreement reviews and updates: other relevant documents or records.

rs-o(o) – Enhancement (Moderate)					
Control					
Access agreements are reviewed and updated a	s part of the system accreditation or when a contract is renewed or extended.				
Applicability: All	References: ARS: PS-6(0); NIST 800-53/53A: PS-6; PISP: 4.13.6	Related Controls:			
ASSESSMENT PROCEDURE: PS-6(0).1					
Assessment Objective					
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.					
Assessment Methods And Objects					

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan (for organization-defined Rev. 9 Page 132 of 189 BPSSM Appendix A, Attachment 2

frequency for access agreem	nent reviews); access agreements; records of access agreement reviews and updates	s; other relevant documents or records.
PS-7 – Third-Party Persor		
Control		
Personnel security controls e provisions for security clearar	employed by external service providers and third parties shall be documented, agreed nces, background checks, required expertise, defined security roles and responsibiliti hall be compliant with CMS IS policies and procedures, and consistent with NIST SP 4	ies, and confidentiality agreements. Personnel security controls employed by service
Guidance		
	e, for example, service bureaus, contractors, and other organizations providing information anagement. The organization explicitly includes personnel security requirements in act.	
Applicability: All	References: ARS: PS-7; IRS-1075: 5.6.2.1#1.8; NIST 800-53/5	i3A: PS-7; PISP: 4.13.7 Related Controls:
ASSESSMENT PROCEDURE	E: PS-7.1	
Assessment Objective		
providing information system (ii) the organization explicitly	es personnel security requirements, including security roles and responsibilities, for the n development, information technology services, outsourced applications, network and rincludes personnel security requirements in acquisition-related documents in accordates third-party provider compliance with personnel security requirements.	d security management);
Assessment Methods And O		
Examine: Personnel security relevant documents or record	y policy; procedures addressing third-party personnel security; list of personnel securi ds.	ity requirements; acquisition documents; compliance monitoring process; other
<u> </u>	ersonnel with personnel security responsibilities; third-party providers.	
PS-7(CMS-1) – Enhancement	t (Moderate)	
5 1	ed to contractors and define security requirements for contractors. Contractors must by requirements. The contractor selection process must assess the contractor's ability	
Applicability: All	References: ARS: PS-7(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE	E: PS-7(CMS-1).1	
providing information system	es personnel security requirements, including security roles and responsibilities, for the development, information technology services, outsourced applications, network and third-party provider compliance with personnel security requirements.	
Examine: Personnel security relevant documents or record	y policy; procedures addressing third-party personnel security; list of personnel securi ds to determine the access provided to contractors and defining security requirements nd support the CMS information security requirements. The contractor selection proc	s for contractors. Contractors must be provided with minimal system and physical
provided with minimal system	ird party security responsibilities to determine that the access provided to contractors n and physical access, and must agree to and support the CMS information security r IS' information security policies, and standards.	are defined within the security requirements for contractors. Contractors must be requirements. The contractor selection process must assess the contractor's ability
PS-8 – Personnel Sanctio	ns (Moderate)	
Control		
	ce formal personnel sanctions process for personnel who fail to comply with establish ws, Executive Orders, policies, directives, regulations, standards, and guidelines.	ed CMS IS policies and procedures. The employee sanction process shall be
Guidance		
•		
personnel policies and procee	nsistent with applicable laws, Executive Orders, directives, policies, regulations, stand adures for the organization.	dards, and guidance. The sanctions process can be included as part of the general

Applicability: All	References: ARS: PS-8; HIPAA: 164.308(a)(1)(ii)(C); NIST 800-53/53A: PS	S-8; PISP: 4.13.8	Related Controls:
ASSESSMENT PROCEDURE: P	S-8.1		
	rmal sanctions process for personnel failing to comply with established information security p ess is consistent with applicable laws, Executive Orders, directives, policies, regulations, star		
Assessment Methods And Obje		hadrae, and guidance.	
	licy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctio	ons; other relevant document	s or records.
	Access during Extraordinary Personnel Circumstances (Moderate)		
Control			
Access to CMS information and in	information systems shall be reviewed during extraordinary personnel circumstances and lim	nited as deemed necessary.	
	sonal problems could be considered extraordinary personal circumstances. For some perso circumstances on a case by case basis.	onnel, recovery from a difficul	t time may take longer than usual and
Applicability: All	References: ARS: PS-9; PISP: 4.13.9		Related Controls:
ASSESSMENT PROCEDURE: PS	S-CMS-1.1		
as deemed necessary. Interview: Organizational person necessary.	licy and procedures; other relevant documents or records determine system access during e nnel with personnel security responsibilities to determine system access during extraordinary	y personnel circumstances is	
PS-CMS-2 – Designate an Inf	formation System Security Officer (ISSO) / System Security Officer (S	SSO) (Moderate)	
Control An Information System Security C	Officer (ISSO) / System Security Officer (SSO) shall be designated for each business compo	onent with roles and responsi	bilities of the position clearly defined.
Guidance A good reference set for defining protect CMS information systems	the Information System Security Officer (ISSO) / System Security Officer (SSO) responsibilis and data.	ities are the NIST SPs. Spec	cific responsibilities should be developed to
Applicability: All	References: ARS: PS-10; FISCAM: TSP-3.1.1, TSP-3.1.2; HIPAA: 164.308	8(a)(2); PISP: 4.13.10	Related Controls:
ASSESSMENT PROCEDURE: P	S-CMS-2.1		
Assessment Methods And Obje	s documented the roles and responsibilities of appointed ISSO / SSO. Acts licy and procedures; other relevant documents or records to determine an ISSO / SSO is des	signated for each component	with roles and responsibilities of the positior

Risk Assessment (RA) - Management

RA-1 – Risk Assessment Policy and Procedures (Moderate)

Control

All CMS applications and systems shall be covered by an IS RA. The RA shall be consistent with NIST SP 800-30. Formal documented procedures shall be developed, disseminated, and reviewed / updated periodically to facilitate the implementation of the RA policy and associated RA controls. The procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-30 provides guidance on the assessment of risk. NIST SP 800-12 provides guidance on security policies and procedures.

	······································			
Applicability: All	References: ARS: RA-1; FISCAM: TAC-3.1.A.2; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075:	Related Controls:		
	5.6.1.1#1.1-2; NIST 800-53/53A: RA-1; PISP: 4.14.1			

ASSESSMENT PROCEDURE: RA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents risk assessment policy and procedures;

(ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization;

- (iii) responsible parties within the organization periodically review risk assessment policy and procedures; and
- (iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.(Optional)

ASSESSMENT PROCEDURE: RA-1.2

Assessment Objective

Determine if:

(i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.(Optional)

RA-2 – Security Categorization (Moderate)

Control

CMS information systems and the information processed, stored, or transmitted by the systems shall be categorized in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to the, CMS System Security Level by Information Type. The security categorization (including supporting rationale) shall be explicitly documented. Designated senior-level officials within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the CMS CIO, CISO, and Business Owners.

All CMS information systems categorized as high or moderate shall be considered sensitive or to contain sensitive information. All CMS information systems categorized as low shall be considered non-sensitive or to contain non-sensitive information. All CMS information systems shall implement minimum security requirements and controls as established in the current CMS IS Standards, based on security categorization of the system.

Guidance

The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST SP 800-60 provides guidance on determining the security categories of the

information types resident on the information system. Applicability: All References: ARS: RA-2; FISCAM: TAC-1.1; HSPD 7: D(8); IRS-1075; 4.1#2; NIST 800-53/53A: RA-Related Controls: MP-4, SC-7 2: PISP: 4.14.2 **ASSESSMENT PROCEDURE: RA-2.1 Assessment Objective** Determine if: (i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners; (ii) the security categorization is consistent with FIPS 199 and NIST SP 800-60; (iii) the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts: (iv) the organization includes supporting rationale for impact-level decisions as part of the security categorization; and (v) designated, senior-level organizational officials review and approve the security categorization of the information system. Assessment Methods And Objects Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST SP 800-60; information system security plan; other relevant documents or records. Interview: Organizational personnel with security categorization and risk assessment responsibilities. RA-3 – Risk Assessment (RA) (Moderate) Control An assessment of risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information systems that support the operations and assets of CMS shall be performed, both within CMS and by external parties that manage / operate information or information systems for CMS. The RA shall be in accordance with current CMS Procedures. Based on the operation of the information system, the RA shall take into account vulnerabilities, threat sources, and security controls in place to determine the resulting level of residual risk posed to CMS operations. CMS assets. CMS information, or individuals. Any findings from reviews of CMS systems shall be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses shall be documented by the Business Owner or external party and addressed by mitigating the risk, accepting the risk with explanation or submitting Corrective Action Plan (CAP). These findings shall be subject to reporting requirements as established by applicable laws. Executive Orders, directives, policies, regulations, standards, and guidance. Guidance Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST SP 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments. Applicability: All References: ARS: RA-3; FISCAM: TAC-3.1.A.2, TSP-1.1.2, TSP-1.1.3, TSP-5.1.4; HIPAA: **Related Controls:** 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3. 6.3.3#2: NIST 800-53/53A: RA-3: PISP: 4.14.3 **ASSESSMENT PROCEDURE: RA-3.1 Assessment Objective** Determine if: (i) the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and (ii) the risk assessment is consistent with the NIST SP 800-30. **Assessment Methods And Objects**

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST SP 800-30; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

RA-3(CMS-1) – Enhancement (Moderate)		
Control		
	t the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessme	ent (RA) Procedures (See CMS Integrated IT
Applicability: All	References: ARS: RA-3(CMS-1); FISCAM: TAC-1.1, TAC-1.2, TSS-2.2.4; HIPAA: 164.306(a)(2); HSPD 7: D(8), F(19)	Related Controls:
ASSESSMENT PROCEDURE: RA-3(CMS-1).		
Assessment Objective	·	
Determine if the organization assesses the risk	and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modif and assets (including information and information systems managed/operated by external parties).	ication, or destruction of information and
Assessment Methods And Objects		
organization-defined frequency for risk assessm	nning policy and procedures; procedures addressing organizational assessments of risk; risk assessment pent updates); records of risk assessment updates; NIST SP 800-30; other relevant documents or record em, and documents the risks and safeguards of the system in accordance with the CMS Information Sec [MEWORK]).	s to determine that prior to project initiation,
safeguards of the system in accordance with the	ssessment responsibilities to determine that prior to project initiation, the organization performs an IS RA e CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Fran	for the system, and documents the risks and nework [FRAMEWORK]).
RA-4 – Risk Assessment Update (Mode	erate)	
Control		
	ery three (3) years or whenever there are significant changes to the system, facilities, or other conditions for re-assessments are listed in section 4.4.6, Security Accreditation.	that may impact the security or accreditation
Guidance		
The organization develops and documents spec updates.	ific criteria for what is considered significant change to the information system. NIST SP 800-30 provides	s guidance on conducting risk assessment
Applicability: All	References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7:	Related Controls:
	F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4	
ASSESSMENT PROCEDURE: RA-4.1	F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4	
Assessment Objective	F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4	
Assessment Objective Determine if:		
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the	
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system;	
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit	assessment updates; It in accordance with the organization-defined frequency or whenever there are significant changes to the pact the security or accreditation status of the system; h the NIST SP 800-30; and	
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit (iv) the revised risk assessment reflects the nee	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system;	
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit (iv) the revised risk assessment reflects the nee Assessment Methods And Objects	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system; h the NIST SP 800-30; and ded changes based on the organization's experiences during security plan implementation.	e information system, the facilities where the
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit (iv) the revised risk assessment reflects the nee Assessment Methods And Objects Examine: Risk assessment policy; security plar	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system; h the NIST SP 800-30; and ded changes based on the organization's experiences during security plan implementation. aning policy and procedures; procedures addressing risk assessment updates; risk assessment; informat	e information system, the facilities where the
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit (iv) the revised risk assessment reflects the nee Assessment Methods And Objects Examine: Risk assessment policy; security plar assessment updates; NIST SP 800-30; other re	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system; h the NIST SP 800-30; and ded changes based on the organization's experiences during security plan implementation. aning policy and procedures; procedures addressing risk assessment updates; risk assessment; informat levant documents or records.	e information system, the facilities where the
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit (iv) the revised risk assessment reflects the nee Assessment Methods And Objects Examine: Risk assessment policy; security plar	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system; h the NIST SP 800-30; and ded changes based on the organization's experiences during security plan implementation. aning policy and procedures; procedures addressing risk assessment updates; risk assessment; informat levant documents or records.	e information system, the facilities where the
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit (iv) the revised risk assessment reflects the nee Assessment Methods And Objects Examine: Risk assessment policy; security plar assessment updates; NIST SP 800-30; other re RA-5 – Vulnerability Scanning (Modera Control Appropriate vulnerability assessment tools and 1 conduct periodic testing of its security posture b appropriate personnel throughout the organizati	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system; h the NIST SP 800-30; and ded changes based on the organization's experiences during security plan implementation. aning policy and procedures; procedures addressing risk assessment updates; risk assessment; informat levant documents or records.	e information system, the facilities where the ion system security plan; records of risk ad maintenance. The organization shall ty scanning process shall be shared with
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessmen system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit (iv) the revised risk assessment reflects the nee Assessment Methods And Objects Examine: Risk assessment policy; security plar assessment updates; NIST SP 800-30; other re RA-5 – Vulnerability Scanning (Modera Control Appropriate vulnerability assessment tools and 1 conduct periodic testing of its security posture b appropriate personnel throughout the organizati	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system; h the NIST SP 800-30; and ded changes based on the organization's experiences during security plan implementation. uning policy and procedures; procedures addressing risk assessment updates; risk assessment; informat levant documents or records. te) techniques shall be implemented by the organization. Selected personnel shall be trained in their use ar y scanning its information systems with vulnerability tools. The information obtained from the vulnerability on on a "need to know" basis to help eliminate similar vulnerabilities in other information systems. The a	e information system, the facilities where the ion system security plan; records of risk ad maintenance. The organization shall ty scanning process shall be shared with
Assessment Objective Determine if: (i) the organization defines the frequency of risk (ii) the organization updates the risk assessment system resides, or other conditions that may imp (iii) the risk assessment update is consistent wit (iv) the revised risk assessment reflects the nee Assessment Methods And Objects Examine: Risk assessment policy; security plar assessment updates; NIST SP 800-30; other re RA-5 – Vulnerability Scanning (Modera Control Appropriate vulnerability assessment tools and t conduct periodic testing of its security posture b appropriate personnel throughout the organizati Internet and email resources shall be subject to Guidance Vulnerability scanning is conducted using appro techniques. Vulnerability scans are scheduled a freely shared with appropriate personnel throug	assessment updates; t in accordance with the organization-defined frequency or whenever there are significant changes to the bact the security or accreditation status of the system; h the NIST SP 800-30; and ded changes based on the organization's experiences during security plan implementation. uning policy and procedures; procedures addressing risk assessment updates; risk assessment; informat levant documents or records. te) techniques shall be implemented by the organization. Selected personnel shall be trained in their use ar y scanning its information systems with vulnerability tools. The information obtained from the vulnerability on on a "need to know" basis to help eliminate similar vulnerabilities in other information systems. The a	e information system, the facilities where the tion system security plan; records of risk and maintenance. The organization shall ty scanning process shall be shared with ctivities of employees using organization

network security testing. NIST SP 800-40 (Versi	on 2) provides guidance on patch and vulnerability management.				
Applicability: All	References: ARS: RA-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5; PISP: 4.14.5	Related Controls:			
ASSESSMENT PROCEDURE: RA-5.1		•			
Assessment Objective					
Determine if:					
(i) the organization defines the frequency of vuln	erability scans within the information system;				
 (ii) the organization scans for vulnerabilities in th and reported; 	e information system in accordance with the organization-defined frequency or when significant new vul	nerabilities affecting the system are identified			
vulnerability management process by using stan	ools and techniques to conduct the vulnerability scans including those tools that ensure interoperability a dards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and male				
procedures, and (c) measuring vulnerability impa	act; ity scanning in accordance with NIST SP 800-42; and				
	lity management in accordance with NIST SP 800-42, and				
Assessment Methods And Objects	iny management in accordance with NIST SP 800-40.				
	deressing wilderschility approximation and information system appretty along wilderschility approxi	na regulta, notab and uningrability			
management records; other relevant documents	ddressing vulnerability scanning; risk assessment; information system security plan; vulnerability scanni	ng results, patch and vulnerability			
o	sessment and vulnerability scanning responsibilities.(Optional)				
RA-5(0) – Enhancement (Moderate)					
Control					
	nd techniques to scan for vulnerabilities in the information system every 90 days or when significant new	vulnerabilities are identified and reported.			
Applicability: All	References: ARS: RA-5(0); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5;	Related Controls:			
· • • • • • • • • • • • • • • • • • • •	PISP: 4.14.5				
ASSESSMENT PROCEDURE: RA-5(0).1					
Assessment Objective					
Determine if the organization meets the requiren	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ying enhancement to the baseline control.			
Assessment Methods And Objects					
	ddressing vulnerability scanning; risk assessment; information system security plan (for organization-de	fined frequency for vulnerability scanning);			
vulnerability scanning results; patch and vulnera	bility management records; other relevant documents or records.				
	sessment and vulnerability scanning responsibilities.(Optional)				
RA-5(CMS-1) – Enhancement (Moderate)					
Control					
	d conduct enterprise security posture review as needed but no less than once a year, in accordance with to Common Vulnerabilities and Exposures (CVE) naming convention.	CMS IS procedures. Document findings and			
Applicability: All	References: ARS: RA-5(CMS-1); HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24)	Related Controls:			
ASSESSMENT PROCEDURE: RA-5(CMS-1).1					
Assessment Objective					
Determine if:					
(i) the organization defines the frequency of vuln					
 (ii) the organization scans for vulnerabilities in th and reported; and 	e information system in accordance with the organization-defined frequency or when significant new vul	nerabilities affecting the system are identified			
	(iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the				
	vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test				
procedures, and (c) measuring vulnerability impa Assessment Methods And Objects	aci.				
	ddressing vulnerability scanning; risk assessment; information system security plan (for organization-de	fined frequency for vulnerability scapping):			
vulnerability scanning results; patch and vulnera	bility management records; other relevant documents or records to determine the organization performs an once a year. Findings are documented and assessment results and vulnerabilities correlate to Comr	penetration testing and conducts enterprise			

naming convention.

Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities to determine the organization performs penetration testing and conducts enterprise security posture review as needed but no less than once a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vulnerabilities and Exposures (CVE) naming convention.

System and Services Acquisition (SA) – Management

SA-1 – System and Services Acquisition Policy and Procedures (Moderate)	
Control	
Documented procedures shall be developed and implemented effectively to facilitate the implementation of the system and services acquisition securit	ty controls in all system and services
acquisitions. Procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
Guidance	
The system and services acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, star	ndards, and guidance. The system and services
acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can	an be developed for the security program in
general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.	
Applicability: All References: ARS: SA-1; IRS-1075: 5.6.1.3#1.1-2; NIST 800-53/53A: SA-1; PISP: 4.15.1	Related Controls:
ASSESSMENT PROCEDURE: SA-1.1	
Assessment Objective	
Determine if:	
(i) the organization develops and documents system and services acquisition policy and procedures;	
(ii) the organization disseminates system and services acquisition policy and procedures to appropriate elements within the organization;	
(iii) responsible parties within the organization periodically review system and services acquisition policy and procedures; and	
(iv) the organization updates system and services acquisition policy and procedures when organizational review indicates updates are required.	
Assessment Methods And Objects	
Examine: System and services acquisition policy and procedures; other relevant documents or records.	
Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)	
ASSESSMENT PROCEDURE: SA-1.2	
Assessment Objective	
Determine if:	
(i) the system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among org	
(ii) the system and services acquisition policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, it	
(iii) the system and services acquisition procedures address all areas identified in the system and services acquisition policy and address achieving policy achieves ac	licy-compliant implementations of all associated
security controls.	
Assessment Methods And Objects	
Examine: System and services acquisition policy and procedures; other relevant documents or records.	
Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)	
SA-1(IRS-1) – Enhancement (Moderate)	
Control	
For FTI, develop, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes IRS d	ocuments received and identified by:
(a) taxpayer name	
(b) tax year(s)	
(c) type of information (e.g., revenue agent reports, Form 1040, work papers)(d) the reason for the request	
(e) date requested	
(f) date received	
(g) exact location of the FTI	
(h) who has had access to the data and	
(i) if disposed of, the date and method of disposition.	
Applicability: All References: IRS-1075: 3.3#1	Related Controls:
ASSESSMENT PROCEDURE: SA-1(IRS-1).1	
Assessment Objective	
Determine if the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition poli	icy that includes IRS documents received and

Rev. 9

identified by:

(a) taxpayer name

(b) tax year(s)

(c) type of information (e.g., revenue agent reports, Form 1040, work papers)

(d) the reason for the request

(e) date requested

(f) date received

(g) exact location of the FTI

(h) who has had access to the data and

(i) if disposed of, the date and method of disposition.

Assessment Methods And Objects

Examine: Organizational documentation that contains the development, dissemination and review/updates to FTI IRS documents received that show:

(a) taxpayer name

(b) tax year(s)

(c) type of information (e.g., revenue agent reports, Form 1040, work papers)

(d) the reason for the request

(e) date requested

(f) date received

(g) exact location of the FTI

(h) who has had access to the data and

(i) if disposed of, the date and method of disposition.

SA-2 – Allocation of Resources (Moderate)

Control

As part of the capital planning and investment control processes, CMS or the external organization shall determine, document, and allocate the resources required to protect CMS information systems adequately. IS requirements shall be included in mission / business case planning, and a separate line item shall be established in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Guidance

The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST SP 800-65 provides guidance on integrating security into the capital planning and investment control process.

v	 0	0			,		 0		
Applicability: All			References: ARS: SA-2: NIST 800-53/53A: SA-2: PISP: 4	4.15.2				Related Controls	:
	 		,,,,,,						
ASSESSMENT PROC	SA-21								

Assessment Objective

Determine if:

(i) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system;

(ii) the organization determines security requirements for the information system in mission/business case planning;

(iii) the organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation; and

(iv) the organization's programming and budgeting process is consistent with NIST SP 800-65.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST SP 800-65; other relevant documents or records. **Interview:** Organizational personnel with capital planning and investment responsibilities.(Optional)

SA-3 – Life Cycle Support (Moderate)

Control

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

Guidance

NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Applicability: All	References: ARS: SA-3; FISCAM: TAY-1.2.1, TCC-1.1.2; NIST 800-53/53A: SA-3; PISP: 4.15.3	Related Controls:
ASSESSMENT PROCEDURE: SA-3.1		

Assessment Objective

Determine if:

(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and

CMS Core Security Requirements for Moderate Impact Level Assessments (ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64. **Assessment Methods And Objects** Examine: System and services acquisition policy: procedures addressing the integration of information security into the system development life cycle process: NIST SP 800-64: information system development life cycle documentation: other relevant documents or records. Interview: Organizational personnel with information security and system life cycle development responsibilities.(Optional) SA-3(CMS-1) – Enhancement (Moderate) Control Must comply with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK. References: ARS: SA-3(CMS-1); FISCAM: TCC-1.1.1 **Related Controls:** Applicability: All ASSESSMENT PROCEDURE: SA-3(CMS-1).1 **Assessment Objective** Determine if: (i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and (ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64. Assessment Methods And Objects Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation; other relevant documents or records to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK. Interview: Organizational personnel with information security and system life cycle development responsibilities to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK. SA-3(FIS-1) – Enhancement (Moderate) Control Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor. Applicability: All References: FISCAM: TCC-2.1.2 **Related Controls:** ASSESSMENT PROCEDURE: SA-3(FIS-1).1 **Assessment Objective** Determine if the organizational detailed system specifications are prepared by the programmer and reviewed by a programming supervisor. **Assessment Methods And Objects** Examine: Design system specifications. Examine: Pertinent policies and procedures. Interview: Programmer and programming supervisor. SA-4 – Acquisitions (Moderate) Control Security requirements and/or security specifications shall be included, either explicitly or by reference, in all information system acquisition contracts based on an assessment of risk in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. Solicitation Documents Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required: 4.15.4.1. Security capabilities; 4.15.4.2. Design and development processes; 4.15.4.3. Test and evaluation procedures; and 4.15.4.4. Documentation. The requirements in the solicitation documents shall permit updating security controls as new threats / vulnerabilities are identified and as new technologies are implemented Use of Evaluated and Validated Products For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to

products that have been evaluated and validated through one or more of the following sources:

rance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme; iteria Recognition Arrangements; and	
Ile Validation Program.	
mentation Guidance	
documentation shall include security configuration settings, including documentation explaining e	exceptions to the standard, and security implementation guidance.
Requests for Proposals) for information systems and services include, either explicitly or by refer	rence, security requirements that describe: (i) required security
as necessary, specific security controls and other specific FISMA requirements); (ii) required desi	ign and development processes; (iii) required test and evaluation
cumentation. The requirements in the solicitation documents permit updating security controls as	
	dance on information technology security services. NIST SP 800-64
nsiderations in the system development life cycle.	
on	
de requirements for appropriate information system documentation. The documentation addresses	
the security controls in the information system. The level of detail required in the documentation is	s based on the FIPS 199 security category for the information
alidated Products	
nce on the acquisition and use of tested/evaluated information technology products.	
mentation Guidance	
	MB FISMA reporting instructions provide guidance on configuration
ion systems. NIST SP 800-70 provides guidance on configuration settings for information technol	logy products.
References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4	Related Controls:
A-4.1	
rity requirements and/or security specifications, either explicitly or by reference, in information system	stem acquisition contracts based on an assessment of risk and in
Executive Orders, directives, policies, regulations, and standards;	
mation systems include, either explicitly or by reference, security requirements and/or security spe	ecifications that describe:
icedures; and	
ucts	
	I/or security specifications into the acquisition process: NIST SP 80
ate)	
quire that appropriate documentation be provided describing the functional properties of the secu ing of the controls.	rity controls employed within the information system with sufficient
	Requests for Proposals) for information systems and services include, either explicitly or by refe as necessary, specific security controls and other specific FISMA requirements); (ii) required des umentation. The requirements in the solicitation documents permit updating security controls as rovides guidance on the selection of information security products. NIST SP 800-35 provides gui insiderations in the system development life cycle. Ion be requirements for appropriate information system documentation. The documentation addresses the security controls in the information system. The level of detail required in the documentation i alidated Products ice on the acquisition and use of tested/evaluated information technology products. Immentation Guidance documentation includes security configuration settings and security implementation guidance. O ion systems. NIST SP 800-70 provides guidance on configuration settings for information techno References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4 A-4.1 urity requirements and/or security specifications, either explicitly or by reference, in information sy Executive Orders, directives, policies, regulations, and standards; of commercial information technology products is consistent with NIST SP 800-23; tration settings and security implementation guidance in organizational acquisitions are consister mation systems include, either explicitly or by reference, security requirements and/or security sp ent processes; coedures; and the processes; coedures; and the processes is include, either explicitly or by reference, other relevant documents or nentation; acquisition contracts for information systems or services; other relevant documents or nel with information system security, acquisition, and contracting responsibilities.(Optional) ate) quire that appropriate documentation be provided describing the functional properties of the securited appropriate documentation be provided describing the functional properties of the securite.

ASSESSMENT PROCEDURE: SA-4(1).1

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.

SA-4(CMS-1) – Enhancement (Moderate)

Control

Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

Applicability: All	References: ARS: SA-4(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SA-4(CMS-1).1		

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records to determine that all contracts and Statements of Work (SOW) that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities to determine that all contracts and SOW that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

SA-5 – Information System Documentation (Moderate)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

Guidance

Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

	Applicability: All	References: ARS: SA-5; FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1, TSD-3.1.2, TSD-3.1.3, TSP- 3.3.2; IRS-1075: 5.6.1.3#1.3; NIST 800-53/53A: SA-5; PISP: 4.15.5	Related Controls:
--	--------------------	--	-------------------

ASSESSMENT PROCEDURE: SA-5.1

Assessment Objective

Determine if:

(i) the organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system;

(ii) the organization makes available information on configuring, installing, and operating the information system; and

(iii) the organization makes available information on effectively using the security features in the information system.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; other relevant documents or records.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.(Optional)

SA-5(1) – Enhancement (Moderate) Control Ensure that system documentation describes the functional properties of the security controls implemented within the information system with sufficient detail to facilitate analysis and testing of the controls. References: ARS: SA-5(1); NIST 800-53/53A: SA-5(1) **Related Controls:** Applicability: All ASSESSMENT PROCEDURE: SA-5(1).1 Assessment Objective Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. **Assessment Methods And Objects** Examine: System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records. Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system. SA-5(CMS-1) – Enhancement (Moderate) Control Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users. References: ARS: SA-5(CMS-1): FISCAM: TSD-1.1.6. TSD-3.1.1 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: SA-5(CMS-1).1 **Assessment Objective** Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). **Assessment Methods And Objects** Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance: and required personnel training to include administrators and users. Interview: Organizational personnel with information system documentation responsibilities: organizational personnel operating, using, and/or maintaining the information system to determine the organization develops system documentation to describe the system's purpose; description; technical operations and access; maintenance; and required personnel training to include administrators and users. SA-5(CMS-2) – Enhancement (Moderate) Control Maintain an updated list of related system operations and security documentation. Applicability: All References: ARS: SA-5(CMS-2); FISCAM: TSD-1.1.6 **Related Controls:** ASSESSMENT PROCEDURE: SA-5(CMS-2).1 **Assessment Objective** Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components). Assessment Methods And Objects Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization maintains an updated list of related system's operations and security documentation. Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization maintains an updated list of related system's operations and security documentation. SA-5(CMS-3) – Enhancement (Moderate) Control Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation. Applicability: All References: ARS: SA-5(CMS-3): FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1 **Related Controls:**

ASSESSMENT PROCEDURE: SA-5(CMS-3).1

Assessment Objective

Determine if responsible parties within the organization periodically review system and services acquisition policy and procedures.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization updates documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine if the organization updates documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation. Refer to "Media Protection" standard for security of hard copies depending on data sensitivity included in the documentation.

SA-5(CMS-4) – Enhancement (Moderate)

Control

Document the system's configuration, and procedures in support of system access administration and operations.

Applicability: All	References: ARS: SA-5(CMS-4); FISCAM: TSD-1.1.6	Related Controls:
ASSESSMENT PROCEDURE: SA-5(CMS-4)	1	

Assessment Objective

Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the requirements for information system documentation; information system documentation including administrator and user guides; other relevant documents or records to determine the organization documents the system's configuration and procedures in support of system access administration and operations. **Interview:** Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system to determine the organization documents the system access administration and procedures in support of system access administration and operations.

SA-5(FIS-1) – Enhancement (Moderate)

Control

Goals are established by senior management on the availability of data processing and on-line services. Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.

Applicability: All	References: FISCAM: TSC-2.4.6, TSC-2.4.9	Related Controls:

ASSESSMENT PROCEDURE: SA-5(FIS-1).1

Assessment Objective

Determine if the organizational goals are established by senior management on the availability of data processing and on-line services. Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation.

Interview: Senior management, data processing management, and user management.

SA-5(FIS-2) – Enhancement (Moderate)

Control

Records are maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.

Applicability: All	References: FISCAM: TSC-2.4.7, TSC-2.4.8	Related Controls:
ASSESSMENT PROCEDURE: SA-5(FIS-2).1		

Assessment Objective

Determine if the organizational records are maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Examine: Supporting documentation. Interview: Senior management, data processing management, and user management. SA-6 – Software Usage Restrictions (Moderate) Control All software or shareware and associated documentation used on CMS information systems shall be deployed and maintained in accordance with appropriate license agreements and copyright laws. Software associated documentation protected by quantity licenses shall be managed through a tracking system to control copying and distribution. All other uses not specifically authorized by the license agreement shall be prohibited. The use of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. Guidance Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. Applicability: All References: ARS: SA-6: FISCAM: TCC-2.3.1: IRS-1075: 4.7.3#1.2: NIST 800-53/53A: SA-6: PISP: **Related Controls:** 4.15.6 **ASSESSMENT PROCEDURE: SA-6.1 Assessment Objective** Determine if: (i) the organization complies with software usage restrictions: and (ii) the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. Assessment Methods And Objects Examine: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records. Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system. (Optional) SA-6(FIS-1) – Enhancement (Moderate) Control Implementation orders, including effective date, are provided to all locations where they are maintained on file. References: FISCAM: TCC-2.3.2 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: SA-6(FIS-1).1 Assessment Objective Determine if the organization provides to all locations software implementation orders, including effective date, where the orders are maintained on file. Assessment Methods And Objects Examine: Implementation orders. Examine: Pertinent policies and procedures. Interview: Information system and security administrators. SA-7 – User Installed Software (Moderate) Control All users shall be restricted from downloading or installing software, unless explicitly authorized in writing by the CIO or his/her designated representative. Users that have been granted such authorization may download and install only organization-approved software. The use of install-on-demand software shall be restricted. Guidance If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect). Applicability: All References: ARS: SA-7; FISCAM: TCC-1.3.1; NIST 800-53/53A: SA-7; PISP: 4.15.7 **Related Controls: ASSESSMENT PROCEDURE: SA-7.1** Assessment Objective Determine if:

(i) the organization enforces explicit rules govern			
(ii) unauthorized software is present on the system; and			
(iii) the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary action.			
Assessment Methods And Objects			
	y; procedures addressing user installed software; list of rules governing user installed software; network	traffic on the information system: other	
relevant documents or records.			
	ation system administration responsibilities; organizational personnel operating, using, and/or maintainin	g the information system.	
	tware on the information system; information system for prohibited software.(Optional)		
SA-7(CMS-1) – Enhancement (Moderate)			
Control			
If user installed software is authorized in writing prohibitions.	by the CIO or his/her designated representative, ensure that business rules and technical controls enforce	e the documented authorizations and	
Applicability: All	References: ARS: SA-7(CMS-1)	Related Controls:	
ASSESSMENT PROCEDURE: SA-7(CMS-1).1			
Assessment Objective			
Determine if:			
(i) the organization enforces explicit rules goverr			
(ii) unauthorized software is present on the syste	em.		
Assessment Methods And Objects			
	y; procedures addressing user installed software; list of rules governing user installed software; network		
	policies exist that ensure business rules and technical controls enforce the documented authorizations a	•	
	ation system administration responsibilities; organizational personnel operating, using, and/or maintainin hnical controls enforce the documented authorizations and prohibitions.	g the mornation system to determine that	
	tware on the information system; information system for prohibited software to determine authorizations	and prohibitions	
SA-8 – Security Engineering Principles			
Control			
	I implemented using accepted security engineering principles.		
Guidance			
NIST SP 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information			
systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to			
	t feasible, given the current state of the hardware, software, and firmware components within the system		
Applicability: All	References: ARS: SA-8; FISCAM: TAY-2.1.1, TAY-2.2.1, TCC-2.1.3; NIST 800-53/53A: SA-8; PISP: 4.15.8	Related Controls:	
ASSESSMENT PROCEDURE: SA-8.1			
Assessment Objective			
Determine if:			
(i) the organization designs and implements the information system using security engineering principles; and			
	inciples in the development and implementation of the information system consistent with NIST SP 800-2	27.	
Assessment Methods And Objects			
	y; procedures addressing security engineering principles used in the development and implementation o		
, ,	rity requirements and security specifications for the information system; other relevant documents or reco	oras.	
SA-8(0) – Enhancement (Moderate)	n and services acquisition responsibilities.(Optional)		
*			
Control			
	sing the security engineering principles detailed in NIST SP 800-27 Rev. A, Engineering Principles for IT		
Applicability: All	References: ARS: SA-8(0); FISCAM: TCC-2.1.3; NIST 800-53/53A: SA-8; PISP: 4.15.8	Related Controls:	
Rev 9	Page 148 of 189	BPSSM Appendix A Attachment 2	

ASSESSMENT PROCEDURE: SA-8(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST SP 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records. Interview: Organizational personnel with system and services acquisition responsibilities.(Optional)

SA-9 – External Information System Services (Moderate)

Control

All external information system services shall include specific provisions requiring the service provider to comply with CMS IS policies, standards, and guidelines; and shall be monitored for compliance. CMS shall define the remedies for any loss, disruption, or damage caused by the service provider's failure to comply. Service providers shall be prohibited from outsourcing any system function overseas, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representatives with concurrence from CMS' personnel security department.

Guidance

An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and response requirements for any identified instance of non-compliance. NIST SP 800-35 provides guidance on the security considerations in the system development life cycle.

Applicability: All	References: ARS: SA-9; FISCAM: TAY-1.3.1; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075:	Related Controls: CA-3
	5.6.1.3#1.4; NIST 800-53/53A: SA-9; PISP: 4.15.9	

ASSESSMENT PROCEDURE: SA-9.1

Assessment Objective

Determine if:

(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;

(ii) the organization monitors security control compliance;

(iii) the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions; and

(iv) the security controls employed by providers of external information system services are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.(Optional)

SA-9(CMS-1) – Enhancement (Moderate)

Control

If service providers are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas, ensure that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Applicability: All References: ARS: SA-9(CMS-1); HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8)	Related Controls:
--	-------------------

ASSESSMENT PROCEDURE: SA-9(CMS-1).1

Assessment Objective

Determine if the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

SA-9(HIP-1) – Enhancement (Moderate)

Control

A covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a).)

Applicability: All	References: HIPAA: 164.308(b)(1), 164.308(b)(4), 164.314(a)(1)(i), 164.314(a)(2)(i),	Related Controls:
	164.314(a)(2)(i)(A), 164.314(a)(2)(i)(B), 164.314(a)(2)(i)(C), 164.314(a)(2)(i)(D),	
	164.314(a)(2)(ii)(A)(1), 164.314(a)(2)(ii)(A)(2), 164.314(a)(2)(ii)(B)	

ASSESSMENT PROCEDURE: SA-9(HIP-1).1

Assessment Objective

Determine if the organizational covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a))

Assessment Methods And Objects

Examine: Organizational documentation meets the requirements set forth in HIPAA regulations (See HIPAA 164.308(b) and 164.314(a)) for a covered entity. Interview: Organizational personnel maintaining covered entity documentation follow requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a).)

SA-10 – Developer Configuration Management (Moderate)

Control

Information system developers shall develop, document, and implement a configuration management plan for each information system under development. The configuration management plan shall address change control mechanisms during development, change authorization requirements, and security flaw identification, tracking, and remediation processes.

Guidance

This control also applies to the development actions associated with information system changes.

Applicability: All	References: ARS: SA-10; NIST 800-53/53A: SA-10; PISP: 4.15.10	Related Controls:
ASSESSMENT PROCEDURE: SA-10.1		

Assessment Objective

Determine if the organization requires that information system developers (and systems integrators) create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records.(Optional)

SA-11 – Developer Security Testing (Moderate)

Control

Information system developers shall develop, document, and implement a security test and evaluation (ST&E) plan for each information system under development in accordance with, but not limited to the, current CMS Procedures. The developer security test results shall be documented.

Guidance

Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant

Applicability: All	References: FISCAM: TCC-2.1.5; NIST 800-53/53A: SA-11	Related Controls: CA-2, CA-4	
ASSESSMENT PROCEDURE	: SA-11.1		
Assessment Objective			
Determine if the organization	requires that information system developers (and systems integrators) create a security test and evalu	uation plan, implement the plan, and document the results.	
Assessment Methods And O	bjects		
	es acquisition policy; procedures addressing information system developer/integrator security testing; ecurity test plans; records of developer/integrator security testing results for the information system; o		
SA-11(CMS-1) – Enhanceme			
Control			
	ation (ST&E) results are used in support of the security C&A process for the information system, ensu	ure that no security relevant modifications of the information	
	sequent to the security testing and after selective verification of the results.	•	
Applicability: All	References: ARS: SA-11(CMS-1); FISCAM: TCC-2.1.8	Related Controls:	
ASSESSMENT PROCEDURE	: SA-11(CMS-1).1		
Assessment Objective			
Determine if the organization	requires that information system developers (and systems integrators) create a security test and evalu	uation plan, implement the plan, and document the results.	
Assessment Methods And Objects			
	es acquisition policy; procedures addressing information system developer/integrator security testing;		
	ecurity test plans; records of developer/integrator security testing results for the information system; o		
	nformation system has been made subsequent to the security testing and after selective verification o	If the results if the security test and evaluation results are used in	
	rocess for the information system.	ions of the information quoter has been made subsequent to the	
	sonnel with developer security testing responsibilities to determine that no security relevant modificati ctive verification of the results if the security test and evaluation results are used in support of the security		
SA-11(CMS-2) – Enhanceme			
Control			
Use hypothetical data when e	vocuting test scripts		
Applicability: All	References: ARS: SI-7(CMS-2)	Related Controls:	
ASSESSMENT PROCEDURE			
Assessment Objective			
	also controls access to areas officially designated as publicly accessible, as appropriate, in accordance	ce with the organization's assessment of risk	
Assessment Methods And O	, , , , , , , , , , , , , , , , , , , ,	se with the organization's assessment of fisk.	
	ation integrity policy; procedures addressing software and information integrity; information system de	sign documentation: information system configuration settings	
	tegrity verification tools and applications documentation; other relevant documents or records to deter		
	stem and information integrity responsibilities to determine hypothetical data is used when executing to		

Interview: Personnel with system and information integrity responsibilities to determine hypothetical data is used when executing test scripts. Test: Information systems to determine hypothetical data is used when executing test scripts.

System and Communications Protection (SC) – Technical

SC-1 – System and Communications Protection Policy and Procedures (Moderate)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: SC-1; FISCAM: TAC-3.2.E.1; IRS-1075: 5.6.3.4#1, 5.6.3.4#2; NIST 800-53/53A: SC-1; PISP: 4.16.1	Related Controls:

ASSESSMENT PROCEDURE: SC-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents system and communications protection policy and procedures;

(ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and

(iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and communications protection responsibilities.(Optional)

ASSESSMENT PROCEDURE: SC-1.2

Assessment Objective

Determine if:

(i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and communications protection responsibilities.(Optional)

SC-2 – Application Partitioning (Moderate)

Control

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Guidance

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Applicability: All	References: ARS: SC-2; NIST 800-53/53A: SC-2; PISP: 4.16.2	Related Controls:
ASSESSMENT PROCEDURE: SC-2.1		

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Separation of user functionality from information system management functionality.(Optional)

SC-2(CMS-1) – Enhancement (Moderate)

Control

Place all CMS servers allowing public access within a DMZ environment, and disallow direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Applicability: All	References: ARS: SC-2(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SC-2(CMS-1).1		

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Interview: Selected organizational personnel with network administration responsibilities to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers. Test: All CMS servers allowing public access to the internal network. DMZ servers can only access these servers within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

SC-3 – Security Function Isolation (Moderate)

Control

Information system security functions shall be isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system shall maintain a separate execution domain (e.g., address space) for each executing process.

Guidance

The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Applicability: All	References: ARS: SC-3; NIST 800-53/53A: SC-3; PISP: 4.16.3	Related Controls:

ASSESSMENT PROCEDURE: SC-3.1

Assessment Objective

Determine if:

(i) the organization defines the security functions of the information system to be isolated from nonsecurity functions; and

(ii) the information system isolates security functions from nonsecurity functions.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Separation of security functions from nonsecurity functions within the information system.(Optional)

SC-4 – Information Remnance (Moderate)

Control

No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.

Guidance

Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

Applicability: All	References: ARS: SC-4; IRS-1075: 5.6.3.4#2; 5.6.3.4#3; NIST 800-53/53A: SC-4; PISP: 4.16.4	Related Controls:

ASSESSMENT PROCEDURE: SC-4.1		
Assessment Objective		
-	nauthorized and unintended information transfer via shared system resources.	
Assessment Methods And Objects	······································	
	tion policy; procedures addressing information remnance; information system design documentatior	n: information system configuration settings and
associated documentation; other relevant docu		, , , , , , , , , , , , , , , , , , , ,
Test: Information system for unauthorized and	unintended transfer of information via shared system resources.(Optional)	
SC-4(0) – Enhancement (Moderate)		
Control		
	cannot intentionally or unintentionally access information remnants, including encrypted representa f a prior user. Ensure that system resources shared between two (2) or more users are released be	
Applicability: All	References: ARS: SC-4(0); IRS-1075: 5.6.3.4#2; NIST 800-53/53A: SC-4; PISP: 4.16.4	Related Controls:
ASSESSMENT PROCEDURE: SC-4(0).1		
Assessment Objective		
-	ments as specified in the baseline control and the specific CMS requirements as prescribed in this	amplifying enhancement to the baseline control
Assessment Methods And Objects	ments as specified in the baseline control and the specific Owo requirements as prescribed in this	ampinying enhancement to the baseline control.
•	tion policy; procedures addressing information remnance; information system design documentatior	n: information system configuration settings and
associated documentation; other relevant docu		n, mormation system configuration settings and
	unintended transfer of information via shared system resources.(Optional)	
SC-4(PII-1) – Enhancement (Moderate)	······································	
Control		
disclosure was made, what was disclosed, and identification will contain the approximate numb transmission.	why and when it was disclosed. Organizations transmitting PII from one computer to another need ber of personal records, the date of the transmissions, the best possible description of the records, a	I only identify the bulk records transmitted. This and the name of the individual making/receiving the
Applicability: All	References: IRS-1075: 3.3#2	Related Controls:
ASSESSMENT PROCEDURE: SC-4(PII-1).1		
Assessment Objective		
reflects to whom the disclosure was made, what transmitted. This identification will contain the a making/receiving the transmission.	rizations for further disclosures (e.g., agents/contractors), information disclosed outside the organiz at was disclosed, and why and when it was disclosed. Organizations transmitting PII from one comp approximate number of personal records, the date of the transmissions, the best possible description	
Assessment Methods And Objects		
Examine: Bulk record identities which have be	en transmitted externally to another organization to determine if the records contain:	
Examine: Bulk record identities which have be • approximate number of personal records		
Examine: Bulk record identities which have be • approximate number of personal records • date of the transmission		
 Examine: Bulk record identities which have been approximate number of personal records date of the transmission best possible description of the records 	en transmitted externally to another organization to determine if the records contain:	
 Examine: Bulk record identities which have been approximate number of personal records date of the transmission best possible description of the records the name of the individuals making/receiving the second se	en transmitted externally to another organization to determine if the records contain:	
Examine: Bulk record identities which have be • approximate number of personal records • date of the transmission • best possible description of the records • the name of the individuals making/receiving the SC-5 – Denial of Service Protection (M	en transmitted externally to another organization to determine if the records contain:	
Examine: Bulk record identities which have bee • approximate number of personal records • date of the transmission • best possible description of the records • the name of the individuals making/receiving to SC-5 – Denial of Service Protection (M Control	en transmitted externally to another organization to determine if the records contain: the transmission. oderate)	
Examine: Bulk record identities which have bee • approximate number of personal records • date of the transmission • best possible description of the records • the name of the individuals making/receiving to SC-5 – Denial of Service Protection (M Control Mechanisms shall be established to prevent, or	en transmitted externally to another organization to determine if the records contain:	
Examine: Bulk record identities which have bee • approximate number of personal records • date of the transmission • best possible description of the records • the name of the individuals making/receiving to SC-5 – Denial of Service Protection (M Control Mechanisms shall be established to prevent, or Guidance	en transmitted externally to another organization to determine if the records contain: the transmission. oderate)	n of the records, and the name of the individual
Examine: Bulk record identities which have bee • approximate number of personal records • date of the transmission • best possible description of the records • the name of the individuals making/receiving to SC-5 – Denial of Service Protection (M Control Mechanisms shall be established to prevent, or Guidance A variety of technologies exist to limit, or in som devices on an organization's internal network fr	en transmitted externally to another organization to determine if the records contain: the transmission. oderate) r limit the effects of well-known, detectable, and preventable denial-of-service attacks. ne cases, eliminate the effects of denial of service attacks. For example, boundary protection device rom being directly affected by denial of service attacks. Information systems that are publicly access	n of the records, and the name of the individual
Examine: Bulk record identities which have bee • approximate number of personal records • date of the transmission • best possible description of the records • the name of the individuals making/receiving to SC-5 – Denial of Service Protection (M Control Mechanisms shall be established to prevent, or Guidance A variety of technologies exist to limit, or in som	en transmitted externally to another organization to determine if the records contain: the transmission. oderate) r limit the effects of well-known, detectable, and preventable denial-of-service attacks. ne cases, eliminate the effects of denial of service attacks. For example, boundary protection device rom being directly affected by denial of service attacks. Information systems that are publicly access	n of the records, and the name of the individual

ASSESSMENT PROCEDURE: SC-5.1		
Assessment Objective		
Determine if:		
	service attacks (or provides references to sources of current denial of service attack	
, , , , , , , , , , , , , , , , , , , ,	nits the effects of the organization-defined or referenced types of denial of service atta	acks.
Assessment Methods And Objects		
Examine: System and communications protection	on policy; procedures addressing denial of service protection; information system des	sign documentation; information system security plan; information
	cumentation; other relevant documents or records.	
	or limitation of the effects of denial of service attacks.(Optional)	
SC-5(0) – Enhancement (Moderate)		
Control		
	al-of-service attacks defined on the following sites or within the following documents:	
 SANS Organization www.sans.org/dosstep; SANS Organization's Roadmap to Defeating D 	DoS www.sans.org/dossten/roadman.php; and	
- NIST CVE List http://checklists.nist.gov/home.c		
Applicability: All	References: ARS: SC-5(0); NIST 800-53/53A: SC-5; PISP: 4.16.5	Related Controls:
ASSESSMENT PROCEDURE: SC-5(0).1		
Assessment Objective		
	nents as specified in the baseline control and the specific CMS requirements as pres	cribed in this amplifying enhancement to the baseline control.
Assessment Methods And Objects		
•	on policy; procedures addressing denial of service protection; information system des	sign documentation; information system security plan (for list of
organization-defined types of denial of service a	ttacks to protect against or limit); information system configuration settings and assoc	ciated documentation; other relevant documents or records.
	or limitation of the effects of denial of service attacks.(Optional)	
SC-5(1) – Enhancement (Moderate)		
Control		
	ervice attacks against other information systems or networks.	
Applicability: All	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1)	Related Controls:
ASSESSMENT PROCEDURE: SC-5(1).1		
Assessment Objective		
Determine if the information system restricts the	ability of users to launch denial of service attacks against other information systems	or networks.
Assessment Methods And Objects		
	on policy; procedures addressing denial of service protection; information system des	sign documentation; information system configuration settings and
associated documentation; other relevant docum		
	or limitation of the effects of denial of service attacks].(Optional)	
SC-5(2) – Enhancement (Moderate)		
Control		
	edundancy to limit the effects of information flooding types of denial of service attacks	
Applicability: All	References: ARS: SC-5(2); NIST 800-53/53A: SC-5(2)	Related Controls:
ASSESSMENT PROCEDURE: SC-5(2).1		
Assessment Objective		
	ccess capacity, bandwidth, or other redundancy to limit the effects of information floor	ding types of denial of service attacks.
Assessment Methods And Objects		
	on policy; procedures addressing denial of service protection; information system des	sign documentation; information system configuration settings and
associated documentation; other relevant docun	ients or records].(Optional)	

SC-6 – Resource Priority (Moderate)

Control

Mechanisms shall be implemented to provide for allocation of information system resources based upon priority. Priority protection shall ensure that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. References: ARS: SC-6: FISCAM: TSC-1.1: NIST 800-53/53A: SC-6: PISP: 4.16.6

Applicability: All

ASSESSMENT PROCEDURE: SC-6.1

Assessment Objective

Determine if the information system limits the use of resources by priority.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing prioritization of information system resources; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

SC-7 – Boundary Protection (Moderate)

Control

Automated boundary protection mechanisms shall be established and supporting procedures shall be developed, documented, and implemented effectively to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces. The operational failure of the boundary protection mechanisms shall not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing site shall provide the same levels of protection as those of the primary site.

Guidance

Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-77 provides guidance on virtual private networks

Applicability: All	References: ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	Related Controls: AC-4, CA-3, MP-4, RA-2

ASSESSMENT PROCEDURE: SC-7.1

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system: and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy: procedures addressing boundary protection: list of key internal boundaries of the information system: information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records. Interview: Selected organizational personnel with boundary protection responsibilities.

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system.(Optional)

SC-7(1) – Enhancement (Moderate)

Control

Physically allocate publicly-accessible information system components (e.g., public web servers, public email servers, public DNS servers) to separate sub-networks with separate physical network

Related Controls:

interfaces.		
Guidance	maganta indude, far avample, publicuuch convers	
	mponents include, for example, public web servers. References: ARS: SC-7(1); NIST 800-53/53A: SC-7(1)	Related Controls:
Applicability: All ASSESSMENT PROCEDURE: SC-7(1).1		Related Controls:
Assessment Objective		
	locates publicly accessible information system components to separate subnetworks with separate	e, physical network interfaces.
Assessment Methods And Objects	rotection policy; procedures addressing boundary protection; information system design documenta	ation: information austam bardware and coffuere.
	on system configuration settings and associated documentation; other relevant documents or recor	
SC-7(2) – Enhancement (Moderate)		
Control		
Prevent public access into the internal net	works except as appropriately mediated.	
Applicability: All	References: ARS: SC-7(2); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(2)	Related Controls:
ASSESSMENT PROCEDURE: SC-7(2).1		
Assessment Objective		
Determine if:		
(i) the organization defines the mediation I	necessary for public access to the organization's internal networks; and	
(ii) the organization prevents public acces	s into the organization's internal networks except as appropriately mediated.	
Assessment Methods And Objects		
Evenue in a Constant and communications as		
	rotection policy; procedures addressing boundary protection; list of mediation vehicles for allowing	
information system design documentation	; boundary protection hardware and software; information system configuration settings and associ	
information system design documentation Test: Automated mechanisms implementi		
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate)	; boundary protection hardware and software; information system configuration settings and associ	
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional)	
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional)	iated documentation; other relevant documents or reco
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional)	
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional)	iated documentation; other relevant documents or reco
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3)	iated documentation; other relevant documents or reco
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the in Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional)	iated documentation; other relevant documents or reco
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the in Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbound access points to the information system to allow for better monitoring of inbound and outbound and outbound and outbound access points to the information system to allow for better monitoring of inbound and outbound and outbound access points to the information system to allow for better monitoring of inbound and outbound and outbound access points to the information system to allow for better monitoring of inbound and outbound and outbound access points to the information system to allow for better monitoring of inbound and outbound access points to the information system to allow for better monitoring of inbound and outbound access points access points to the information system to allow for better monitoring of inbound and outbound access points access points to the information system to allow for better monitoring of inbound and outbound access points	Related Controls:
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the in Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications pro-	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbourd and outbourd retwork traffic. rotection policy; procedures addressing boundary protection; information system design documentation and access and addressing boundary protection; information system design documentation and access points to the information system to allow for better monitoring of inbound and outbourd and outbourd and outbourd protection; information system design documentation access points and addressing boundary protection; information system design documentation access points and addressing boundary protection; information system design documentation access points access addressing boundary protection; information system design documentation access points access addressing boundary protection; information system design documentation access access access access access and access ac	Related Controls:
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the nur Assessment Methods And Objects Examine: System and communications pri information system architecture and config	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbound access points to the information system to allow for better monitoring of inbound and outbound and outbound and outbound access points to the information system to allow for better monitoring of inbound and outbound and outbound access points to the information system to allow for better monitoring of inbound and outbound and outbound access points to the information system to allow for better monitoring of inbound and outbound and outbound access points to the information system to allow for better monitoring of inbound and outbound access points to the information system to allow for better monitoring of inbound and outbound access points access points to the information system to allow for better monitoring of inbound and outbound access points access points to the information system to allow for better monitoring of inbound and outbound access points	Related Controls:
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications pr information system architecture and config SC-7(4) – Enhancement (Moderate)	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbourd and outbourd retwork traffic. rotection policy; procedures addressing boundary protection; information system design documentation and access and addressing boundary protection; information system design documentation and access points to the information system to allow for better monitoring of inbound and outbourd and outbourd and outbourd protection; information system design documentation access points and addressing boundary protection; information system design documentation access points and addressing boundary protection; information system design documentation access points access addressing boundary protection; information system design documentation access points access addressing boundary protection; information system design documentation access access access access access and access ac	Related Controls:
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications pr information system architecture and config SC-7(4) – Enhancement (Moderate) Control	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional)	Related Controls:
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications pr information system architecture and config SC-7(4) – Enhancement (Moderate) Control Maintain a managed interface with any ex	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbourd and outbourd retwork traffic. rotection policy; procedures addressing boundary protection; information system design documenta	Related Controls:
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications pr information system architecture and config SC-7(4) – Enhancement (Moderate) Control	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbourd network traffic. rotection policy; procedures addressing boundary protection; information system design documentation; or documentation; information system configuration settings and associated documentation; or documentation; information service, implementing controls appropriate to the required protection of the ternal telecommunication service, implementing controls appropriate to the required protection of the ternal telecommunication service, implementing controls appropriate to the required protection of the ternal telecommunication service.	Related Controls:
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the in Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications pr information system architecture and config SC-7(4) – Enhancement (Moderate) Control Maintain a managed interface with any ex transmitted. Applicability: All	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbourd and outbourd network traffic access points to the information system to allow for better monitoring of inbound and outbourd and outbourd and outbourd and outbourd protection policy; procedures addressing boundary protection; information system design documentation documentation; information system configuration settings and associated documentation; of the ternal telecommunication service, implementing controls appropriate to the required protection of the References: ARS: SC-7(4); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(4)	Related Controls: Related Controls: bund network traffic. ation; boundary protection hardware and software; other relevant documents or records. he confidentiality and integrity of the information being
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications prinformation system architecture and config SC-7(4) – Enhancement (Moderate) Control Maintain a managed interface with any exit transmitted. Applicability: All ASSESSMENT PROCEDURE: SC-7(4).1	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbourd and outbourd network traffic access points to the information system to allow for better monitoring of inbound and outbourd and outbourd and outbourd and outbourd protection policy; procedures addressing boundary protection; information system design documentation documentation; information system configuration settings and associated documentation; of the ternal telecommunication service, implementing controls appropriate to the required protection of the References: ARS: SC-7(4); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(4)	Related Controls: Related Controls: bund network traffic. ation; boundary protection hardware and software; other relevant documents or records. he confidentiality and integrity of the information being
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications prinformation system architecture and config SC-7(4) – Enhancement (Moderate) Control Maintain a managed interface with any exit transmitted. Applicability: All ASSESSMENT PROCEDURE: SC-7(4).1 Assessment Objective	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbourd and outbourd network traffic access points to the information system to allow for better monitoring of inbound and outbourd and outbourd and outbourd and outbourd protection policy; procedures addressing boundary protection; information system design documentation documentation; information system configuration settings and associated documentation; of the ternal telecommunication service, implementing controls appropriate to the required protection of the References: ARS: SC-7(4); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(4)	Related Controls: Related Controls: bund network traffic. ation; boundary protection hardware and software; other relevant documents or records. he confidentiality and integrity of the information being
information system design documentation Test: Automated mechanisms implementi SC-7(3) – Enhancement (Moderate) Control Limit the number of access points to the ir Applicability: All ASSESSMENT PROCEDURE: SC-7(3).1 Assessment Objective Determine if the organization limits the num Assessment Methods And Objects Examine: System and communications prinformation system architecture and config SC-7(4) – Enhancement (Moderate) Control Maintain a managed interface with any exit transmitted. Applicability: All ASSESSMENT PROCEDURE: SC-7(4).1 Assessment Objective Determine if:	; boundary protection hardware and software; information system configuration settings and associng access controls for public access to the organization's internal networks.(Optional) formation system to allow for better monitoring of inbound and outbound network traffic. References: ARS: SC-7(3); NIST 800-53/53A: SC-7(3) mber of access points to the information system to allow for better monitoring of inbound and outbourd and outbourd network traffic access points to the information system to allow for better monitoring of inbound and outbourd and outbourd and outbourd and outbourd protection policy; procedures addressing boundary protection; information system design documentation documentation; information system configuration settings and associated documentation; of the ternal telecommunication service, implementing controls appropriate to the required protection of the References: ARS: SC-7(4); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(4)	Related Controls: Dund network traffic. ation; boundary protection hardware and software; other relevant documents or records. he confidentiality and integrity of the information being Related Controls:

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software: information system architecture and configuration documentation: information system configuration settings and associated documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.(Optional)

SC-7(5) – Enhancement (Moderate) Control Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required. Applicability: All References: ARS: SC-7(5); FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-7(5) **Related Controls:** ASSESSMENT PROCEDURE: SC-7(5).1 **Assessment Objective** Determine if the information system denies network traffic by default and allows network traffic by exception. **Assessment Methods And Objects** Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation: other relevant documents or records. Interview: Selected organizational personnel with boundary protection responsibilities.(Optional) SC-7(CMS-1) – Enhancement (Moderate) Control Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. Applicability: All References: ARS: SC-7(CMS-1) **Related Controls:** ASSESSMENT PROCEDURE: SC-7(CMS-1).1 **Assessment Objective** Determine if: (i) the organization defines key internal boundaries of the information system; and (ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. Assessment Methods And Objects Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. Interview: Selected organizational personnel with boundary protection responsibilities to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system: and automated mechanisms implementing boundary protection capability within the information system to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. SC-7(CMS-2) – Enhancement (Moderate) Control Utilize stateful inspection / application firewall hardware and software. References: ARS: SC-7(CMS-2): FISCAM: TAC-3.2.E.1 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: SC-7(CMS-2).1 **Assessment Objective** Determine if: (i) the organization defines key internal boundaries of the information system; and (ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. **Assessment Methods And Objects** Examine: System and communications protection policy: procedures addressing boundary protection: list of key internal boundaries of the information system: information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes stateful inspection / application firewall hardware and software.

SC-7(CMS-3) – Enhancem	rotection capability within the information system to determine if the organization utilizes stateful inspenent (Moderate)	
Control		
	ast two (2) different vendors at the various levels within the network to reduce the possibility of compro	omising the entire network.
pplicability: All	References: ARS: SC-7(CMS-3)	Related Controls:
SSESSMENT PROCEDU		
ssessment Objective		
	tion defines key internal boundaries of the information system.	
ssessment Methods And		
documentation; boundary organization utilizes firewa Interview: Selected orgar within the network to reduc Test: Information system implementing boundary pr	Immunications protection policy; procedures addressing boundary protection; list of key internal bound protection hardware and software; information system configuration settings and associated documer alls from at least two (2) different vendors at the various levels within the network to reduce the possib nizational personnel with boundary protection responsibilities to determine if the organization utilizes fi ice the possibility of compromising the entire network. monitoring and control of communications at the external boundary of the information system and at k rotection capability within the information system to determine if the organization utilizes firewalls from ssibility of compromising the entire network.	ntation; and other relevant documents or records to determine if the ility of compromising the entire network. rewalls from at least two (2) different vendors at the various levels rey internal boundaries within the system; automated mechanisms
C-8 – Transmission In		
ontrol		
	loped and documented, and technical controls shall be established and implemented effectively to pro	tect the integrity of CMS information while in transit.
uidance		
	ng on a commercial service provider for transmission services as a commodity item rather than a fully	
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don	implementation of needed security controls for transmission integrity. When it is infeasible or impraction or propriate contracting vehicles, the organization either implements appropriate compensating security or tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contaits and the security verification.	cal to obtain the necessary security controls and assurances of controntrols or explicitly accepts the additional risk. NIST SP 800-52 e on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems.
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All	implementation of needed security controls for transmission integrity. When it is infeasible or impraction or priate contracting vehicles, the organization either implements appropriate compensating security or tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS	cal to obtain the necessary security controls and assurances of controntrols or explicitly accepts the additional risk. NIST SP 800-52 e on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems.
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All	implementation of needed security controls for transmission integrity. When it is infeasible or impraction or priate contracting vehicles, the organization either implements appropriate compensating security or tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS	cal to obtain the necessary security controls and assurances of controntrols or explicitly accepts the additional risk. NIST SP 800-52 e on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems.
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All SSESSMENT PROCEDU ssessment Objective	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security categority transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1	cal to obtain the necessary security controls and assurances of controntrols or explicitly accepts the additional risk. NIST SP 800-52 e on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems.
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security of tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information.	cal to obtain the necessary security controls and assurances of controntrols or explicitly accepts the additional risk. NIST SP 800-52 e on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems.
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatio ssessment Methods And	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security categories that the organization either implements appropriate compensating security categories that the organization either implements appropriate compensating security categories that the organization either implements appropriate compensating security categories that the organization either implements appropriate compensating security categories that the organization either implements appropriate compensating security categories that the organization either implements appropriate compensating security categories the integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains and integrity verification. NSTISSI No. 7003 contains are set to the securities the integrity of transmitted information. d Objects	cal to obtain the necessary security controls and assurances of cont ontrols or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Dom pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatio ssessment Methods And Examine: System and con	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security of tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects mmunications protection policy; procedures addressing transmission integrity; information system des	cal to obtain the necessary security controls and assurances of cont ontrols or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security of tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects mmunications protection policy; procedures addressing transmission integrity; information system des n; other relevant documents or records.	cal to obtain the necessary security controls and assurances of controls or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation Test: Transmission integri	implementation of needed security controls for transmission integrity. When it is infeasible or impraction or priate contracting vehicles, the organization either implements appropriate compensating security created in the transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects mmunications protection policy; procedures addressing transmission integrity; information system des in; other relevant documents or records. rity capability within the information system.(Optional)	cal to obtain the necessary security controls and assurances of cont ontrols or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation Test: Transmission integri C-8(1) – Enhancement (N	implementation of needed security controls for transmission integrity. When it is infeasible or impraction or priate contracting vehicles, the organization either implements appropriate compensating security created in the transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects mmunications protection policy; procedures addressing transmission integrity; information system des in; other relevant documents or records. rity capability within the information system.(Optional)	cal to obtain the necessary security controls and assurances of contronation on the second se
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Dom pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation Test: Transmission integri C-8(1) – Enhancement (Montrol	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security of tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS IRE: SC-8.1 on system protects the integrity of transmitted information. d Objects ommunications protection policy; procedures addressing transmission integrity; information system des n; other relevant documents or records. rity capability within the information system.(Optional) Moderate)	cal to obtain the necessary security controls and assurances of cont ontrols or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Dom oplicability: All SSESSMENT PROCEDU sessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation Test: Transmission integri C-8(1) – Enhancement (No ontrol Employ approved cryptoge	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security categories to the organization either implements appropriate compensating security categories to the organization either implements appropriate compensating security categories to the organization either implements appropriate compensating security categories to the organization either implements appropriate compensating security categories to the organization either implements appropriate compensating security categories to the organization either implements appropriate compensating security categories the organization integrity verification. NSTISSI No. 7003 contains in Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains in the second se	cal to obtain the necessary security controls and assurances of cont ontrols or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don oplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation Test: Transmission integri C-8(1) – Enhancement (No ontrol Employ approved cryptogi oplicability: All	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security cate tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects ommunications protection policy; procedures addressing transmission integrity; information system des n; other relevant documents or records. rity capability within the information system.(Optional) Moderate) praphic mechanisms to ensure recognition of changes to information during transmission. References: ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312	cal to obtain the necessary security controls and assurances of cont ontrols or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Dom pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and cor associated documentation Test: Transmission integri C-8(1) – Enhancement (N ontrol Employ approved cryptogr pplicability: All SSESSMENT PROCEDU	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security cate tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects ommunications protection policy; procedures addressing transmission integrity; information system des n; other relevant documents or records. rity capability within the information system.(Optional) Moderate) praphic mechanisms to ensure recognition of changes to information during transmission. References: ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312	cal to obtain the necessary security controls and assurances of cont ontrols or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on prot provides guidance on Dom pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation Test: Transmission integri C-8(1) – Enhancement (N ontrol Employ approved cryptogr pplicability: All SSESSMENT PROCEDU ssessment Objective	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security of tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects ommunications protection policy; procedures addressing transmission integrity; information system des n; other relevant documents or records. rity capability within the information system.(Optional) Moderate) praphic mechanisms to ensure recognition of changes to information during transmission. References: ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312 JRE: SC-8(1).1	cal to obtain the necessary security controls and assurances of cont ontrols or explicitly accepts the additional risk. NIST SP 800-52 te on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls: ign documentation; information system configuration settings and 2(c)(1) Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Dom pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation Test: Transmission integri C-8(1) – Enhancement (N ontrol Employ approved cryptogr pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security of tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects mmunications protection policy; procedures addressing transmission integrity; information system des n; other relevant documents or records. rity capability within the information system.(Optional) Moderate) praphic mechanisms to ensure recognition of changes to information during transmission. References: ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312 JRE: SC-8(1).1 on system employs cryptographic mechanisms to recognize changes to information during transmission	cal to obtain the necessary security controls and assurances of controls or explicitly accepts the additional risk. NIST SP 800-52 is on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls: ign documentation; information system configuration settings and 2(c)(1) Related Controls:
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Dom pplicability: All SSESSMENT PROCEDU SSESSMENT Objective Determine if the information SSESSMENT Methods And Examine: System and con associated documentation Test: Transmission integri C-8(1) – Enhancement (N Sontrol Employ approved cryptogr pplicability: All SSESSMENT PROCEDU SSESSMENT PROCEDU SSESSMENT PROCEDU SSESSMENT Objective Determine if the information SSESSMENT Methods And	implementation of needed security controls for transmission integrity. When it is infeasible or impraction or priate contracting vehicles, the organization either implements appropriate compensating security of tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contai References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS IRE: SC-8.1 on system protects the integrity of transmitted information. d Objects mmunications protection policy; procedures addressing transmission integrity; information system des n; other relevant documents or records. rity capability within the information system.(Optional) Moderate) praphic mechanisms to ensure recognition of changes to information during transmission. References: ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312 IRE: SC-8(1).1 on system employs cryptographic mechanisms to recognize changes to information during transmission. d Objects	cal to obtain the necessary security controls and assurances of contoner of explicitly accepts the additional risk. NIST SP 800-52 are on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls: ign documentation; information system configuration settings and 2(c)(1) Related Controls: on unless otherwise protected by alternative physical measures
assurances regarding the effectiveness through app provides guidance on prot provides guidance on Don pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con associated documentation Test: Transmission integri C-8(1) – Enhancement (N ontrol Employ approved cryptog pplicability: All SSESSMENT PROCEDU ssessment Objective Determine if the informatic ssessment Methods And Examine: System and con	implementation of needed security controls for transmission integrity. When it is infeasible or impraction propriate contracting vehicles, the organization either implements appropriate compensating security of tecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance main Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contain References: ARS: SC-8; HIPAA: 164.312(c)(1); NIST 800-53/53A: SC-8; PIS JRE: SC-8.1 on system protects the integrity of transmitted information. d Objects mmunications protection policy; procedures addressing transmission integrity; information system des n; other relevant documents or records. rity capability within the information system.(Optional) Moderate) praphic mechanisms to ensure recognition of changes to information during transmission. References: ARS: SC-8(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312 JRE: SC-8(1).1 on system employs cryptographic mechanisms to recognize changes to information during transmission	cal to obtain the necessary security controls and assurances of conton ontrols or explicitly accepts the additional risk. NIST SP 800-52 te on protecting transmission integrity using IPSec. NIST SP 800-81 ns guidance on the use of Protective Distribution Systems. P: 4.16.8 Related Controls: tign documentation; information system configuration settings and 2(c)(1) Related Controls: on unless otherwise protected by alternative physical measures

SC-8(CMS-1) – Enhancement (Moderate)		
Control		
Employ appropriate approved mechanisms (e.g., SC-13, Use of Cryptography, PISP 4.16.13).	digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to de	estination outside of a secured network (see
Applicability: All	References: ARS: SC-8(CMS-1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(c)(1), 164.312(e)(2)(i)	Related Controls: SC-13
ASSESSMENT PROCEDURE: SC-8(CMS-1).1		
Assessment Objective		
Determine if the information system protects the	integrity of transmitted information.	
Assessment Methods And Objects		
associated documentation; and other relevant do protect the integrity of data while in transit from s Interview: Network administrators to determine i	In policy; procedures addressing transmission integrity; information system design documentation; inform ocuments or records to determine if the organization employs appropriate approved mechanisms (e.g., d ource to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13). f the organization employs appropriate approved mechanisms (e.g., digital signatures, cryptographic has cured network (see SC-13, Use of Cryptography, PISP 4.16.13).	ligital signatures, cryptographic hashes) to
Test: Transmission integrity capability within the	information system to determine if the organization employs appropriate approved mechanisms (e.g., dig ource to destination outside of a secured network (see SC-13, Use of Cryptography, PISP 4.16.13).	gital signatures, cryptographic hashes) to
SC-9 – Transmission Confidentiality (Me		
Control		
	, and technical controls shall be established and implemented effectively to protect the confidentiality of (CMS sensitive information while in transit.
assurances regarding the implementation of nee control effectiveness through appropriate contract	vice provider for transmission services as a commodity item rather than a fully dedicated service, it may lead security controls for transmission confidentiality. When it is infeasible or impractical to obtain the nect sting vehicles, the organization either implements appropriate compensating security controls or explicitly nfidentiality using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting trans-	essary security controls and assurances of accepts the additional risk. NIST SP 800-52
Applicability: All	References: ARS: SC-9; HIPAA: 164.312(e)(1); IRS-1075: 5.6.3.4#2, 5.6.3.4#4.1; NIST 800-53/53A: SC-9; PISP: 4.16.9	Related Controls: AC-17
ASSESSMENT PROCEDURE: SC-9.1		
Assessment Objective		
Determine if the information system protects the	confidentiality of transmitted information.	
Assessment Methods And Objects		
Examine: System and communications protection information system configuration settings and as Test: Transmission confidentiality capability with	n policy; procedures addressing transmission confidentiality; information system design documentation; sociated documentation; other relevant documents or records.	contracts for telecommunications services;
SC-9(1) – Enhancement (Moderate)		
Control Encryption is not required within a secured network. When transmitting data outside of a secured network: (a) An approved encryption method must be used (see SC-13, Use of Cryptography, PISP 4.16.13) (see SC-CMS-4 for E-Mail), and (b) Either a VPN or dedicated leased lines/circuits must be used.		
Applicability: All	References: ARS: SC-9(1); FISCAM: TAC-3.2.E.1, TAC-3.3; HIPAA: 164.312(e)(1), 164.312(e)(2)(ii); IRS-1075: 5.6.3.4#2, 5.7#1	Related Controls: SC-13
ASSESSMENT PROCEDURE: SC-9(1).1		
Assessment Objective		
-	otographic mechanisms to prevent unauthorized disclosure of information during transmission unless oth	erwise protected by alternative physical

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Cryptographic mechanisms implementing transmission confidentiality capability within the information system. (Optional)

SC-9(PII-1) – Enhancement (Moderate)

Control

When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Applicability: All	References: IRS-1075: 5.7.4#1	Related Controls:
ASSESSMENT PROCEDURE: SC-9(PII-1).1		

Assessment Objective

Determine if the organization sending and receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Assessment Methods And Objects

Examine: Fax machine locations for secure custodial coverage of outgoing and incoming PII transmitted data.

Test: Send or receive a simulated PII fax to ensure that:

(i) a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines is located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients is maintained; and (iii) a cover sheet is used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

SC-10 – Network Disconnect (Moderate)

Control

Technical controls shall be established and implemented effectively to ensure that network connections are properly terminated at the end of user sessions, or upon the occurrence of specified conditions (e.g., a period of inactivity).

Guidance

The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Applicability: All	References: ARS: SC-10; NIST 800-53/53A: SC-10; PISP: 4.16.10	Related Controls:

ASSESSMENT PROCEDURE: SC-10.1

Assessment Objective

Determine if:

(i) the organization defines the time period of inactivity before the information system terminates a network connection; and

(ii) the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.

Test: Network disconnect capability within the information system.

SC-10(0) – Enhancement (Moderate)

Control

Configure the information system to forcibly disconnect network connections at the end of a session, or after fifteen (15) minutes of inactivity, for mainframe sessions.

Applicability: All	References: ARS: SC-10(0); FISCAM: TAC-3.2.C.3; NIST 800-53/53A: SC-10; PISP: 4.16.10	Related Controls:

ASSESSMENT PROCEDURE: SC-10(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect: information system configuration settings and associated documentation; other relevant documents or records. Test: Network disconnect capability within the information system. SC-11 – Trusted Path (Moderate) Control Technical controls shall be established and implemented effectively to provide the capability to establish trusted communications paths between authorized users and the security functionality of the information system. Guidance A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login). References: ARS: SC-11: NIST 800-53/53A: SC-11: PISP: 4.16.11 **Related Controls:** Applicability: All **ASSESSMENT PROCEDURE: SC-11.1 Assessment Objective** Determine if: (i) the organization defines the security functions within the information system that are included in a trusted communications path; (ii) the organization-defined security functions include information system authentication and reauthentication; and (iii) the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system. **Assessment Methods And Objects** Examine: System and communications protection policy: procedures addressing trusted communications paths; information system security plan; information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records. (Optional) Test: Automated mechanisms implementing trusted communications paths within the information system. (Optional) SC-11(0) – Enhancement (Moderate) Control At a minimum, a trusted communications path is established between the user and the following system security functions: system authentication, re-authentication, and key management. References: ARS: SC-11(0); FISCAM: TAC-3.2.E.1; PISP: 4.16.11 **Related Controls:** Applicability: All ASSESSMENT PROCEDURE: SC-11(0).1 **Assessment Objective** Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** Examine: System and communications protection policy; procedures addressing trusted communications paths; information system security plan (for organization-defined security functions to include for authentication and reauthentication); information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records. Test: Automated mechanisms implementing trusted communications paths within the information system. SC-12 – Cryptographic Key Establishment and Management (Moderate) Control When cryptography is required and used within the information system, documented procedures shall be implemented effectively for cryptographic key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect sensitive information shall be controlled and distributed using the NIST SP 800-56 and NIST SP 800-57 approved key management quidance. Guidance NIST SP 800-56 provides guidance on cryptographic key establishment. NIST SP 800-57 provides guidance on cryptographic key management. References: ARS: SC-12: IRS-1075: 5.7.1#1: NIST 800-53/53A: SC-12: PISP: 4.16.12 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: SC-12.1 **Assessment Objective** Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system. **Assessment Methods And Objects** Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST SP 800-56 and 800-57; information system design Page 162 of 189 BPSSM Appendix A, Attachment 2 Rev. 9

documentation; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with responsibilities for cryptographic key establishment or management.(Optional)

Test: Automated mechanisms implementing cryptographic key management and establishment within the information system.(Optional)

SC-12(CMS-1) – Enhancement (Moderate)

Control

Employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall prohibit the use of encryption keys that are not recoverable by authorized personnel, require senior management approval to authorize recovery of keys by other than the key owner, and comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Applicability: All	References: ARS: SC-12(CMS-1)	Related Controls: MA-CMS-1, MA-CMS-2,
		SC-13

ASSESSMENT PROCEDURE: SC-12(CMS-1).1

Assessment Objective

Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Interview: A sample of organizational personnel with responsibilities for cryptographic key establishment or management to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Test: Automated mechanisms implementing cryptographic key management and establishment within the information system to determine if the organization employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. The mechanisms and procedures shall comply with approved cryptography standards (see SC-13, Use of Cryptography, PISP 4.16.13).

SC-13 – Use of Cryptography (Moderate)

Control

When cryptographic mechanisms are used, procedures shall be developed, documented, and implemented effectively to ensure they comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. All such mechanisms shall be FIPS 140-2 (as amended and revised) compliant and NIST validated.

Guidance

The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	References: ARS: SC-13; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2,	Related Controls: AC-17(CMS-1), AC-
	5.6.3.4#4.2-3; NIST 800-53/53A: SC-13; PISP: 4.16.13	19(CMS-1), AC-3, AC-3(CMS-1), MP-
		4(PII-1), SC-12(CMS-1), SC-8(CMS-1),
		SC-9(1)

ASSESSMENT PROCEDURE: SC-13.1

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

SC-14 – Public Access Protections (Moderate)

Control

Technical controls shall be developed, documented, and implemented effectively to protect the integrity of the publicly accessible CMS information and applications.

Applicability: All ASSESSMENT PROCEDURE: SO	References: ARS: SC-14; NIST 800-53/53A: SC-14; PISP: 4.16.14	Related Controls:
ASSESSIVIENT PROCEDURE: SU		
Assessment Objective		
•	em protects the integrity and availability of publicly available information and applications.	
Assessment Methods And Object		
	ations protection policy; procedures addressing public access protections; access control policy an	nd procedures: boundary protection procedures: information
	formation system configuration settings and associated documentation; other relevant documents of	
Test: Automated mechanisms imp	plementing access controls and boundary protection for publicly available information and applicati	tions within the information system.(Optional)
SC-14(CMS-1) – Enhancement (M	Moderate)	
Control		
	rols, operating system file permissions, and application configurations protect the integrity of inform	nation stored, processed, and transmitted by publicly accessible
systems, as well as the integrity o		
Applicability: All	References: ARS: SC-14(CMS-1); FISCAM: TAC-3.2.E.1	Related Controls:
ASSESSMENT PROCEDURE: SO	C-14(CMS-1).1	
Assessment Objective		
Determine if the information syste	em protects the integrity and availability of publicly available information and applications.	
Assessment Methods And Object	cts	
	ations protection policy; procedures addressing public access protections; access control policy an	
	formation system configuration settings and associated documentation; and other relevant docume	
accessible applications.	ication configurations protect the integrity of information stored, processed, and transmitted by pub	blicly accessible systems, as well as the integrity of publicly
	nel to determine if network access controls, operating system file permissions, and application con	figurations protect the integrity of information stored, processed
	sible systems, as well as the integrity of publicly accessible applications.	ingurations protect the integrity of information stored, processed
Test: Interfaces for all public-facir	ng networks to determine if network access controls, operating system file permissions, and applica	ation configurations protect the integrity of information stored,
processed, and transmitted by pu	blicly accessible systems, as well as the integrity of publicly accessible applications.	ation configurations protect the integrity of information stored,
	blicly accessible systems, as well as the integrity of publicly accessible applications.	ation configurations protect the integrity of information stored,
processed, and transmitted by pu	blicly accessible systems, as well as the integrity of publicly accessible applications.	ation configurations protect the integrity of information stored,
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (I Control	Iblicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A	
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All	blicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A References: ARS: SC-14(CMS-2)	
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All	blicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A References: ARS: SC-14(CMS-2)	for e-Authentication Standards.
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC	blicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A References: ARS: SC-14(CMS-2)	for e-Authentication Standards.
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste	biblicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A i References: ARS: SC-14(CMS-2) C-14(CMS-2).1 em protects the integrity and availability of publicly available information and applications.	for e-Authentication Standards.
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object	bilicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A i References: ARS: SC-14(CMS-2) C-14(CMS-2).1 em protects the integrity and availability of publicly available information and applications. cts	for e-Authentication Standards. Related Controls:
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object Examine: System and communic	blicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A i References: ARS: SC-14(CMS-2) C-14(CMS-2).1 em protects the integrity and availability of publicly available information and applications. cts cations protection policy; procedures addressing public access protections; access control policy ar	for e-Authentication Standards. Related Controls: nd procedures; boundary protection procedures; information
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object Examine: System and communic system design documentation; inf	biblicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A i References: ARS: SC-14(CMS-2) C-14(CMS-2).1 em protects the integrity and availability of publicly available information and applications. cts cations protection policy; procedures addressing public access protections; access control policy ar formation system configuration settings and associated documentation; and other relevant docume	for e-Authentication Standards. Related Controls: nd procedures; boundary protection procedures; information
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object Examine: System and communic system design documentation; inf implemented in conjunction with c	biblicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A i References: ARS: SC-14(CMS-2) C-14(CMS-2).1 em protects the integrity and availability of publicly available information and applications. cts cations protection policy; procedures addressing public access protections; access control policy ar formation system configuration settings and associated documentation; and other relevant docume or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.	for e-Authentication Standards. Related Controls: nd procedures; boundary protection procedures; information ents or records to determine if e-authentication is required and
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object Examine: System and communic system design documentation; inf implemented in conjunction with c Interview: MA owners for each pu	biblicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A i References: ARS: SC-14(CMS-2) C-14(CMS-2).1 em protects the integrity and availability of publicly available information and applications. cts cations protection policy; procedures addressing public access protections; access control policy ar formation system configuration settings and associated documentation; and other relevant docume	for e-Authentication Standards. Related Controls: nd procedures; boundary protection procedures; information ents or records to determine if e-authentication is required and
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object Examine: System and communic system design documentation; inf implemented in conjunction with content of the information of the Interview: MA owners for each pu e-Authentication Standards.	billicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) Implemented in conjunction with or related to public access protections, refer to ARS Appendix A in References: ARS: SC-14(CMS-2) C-14(CMS-2).1 em protects the integrity and availability of publicly available information and applications. cts cations protection policy; procedures addressing public access protections; access control policy are formation system configuration settings and associated documentation; and other relevant docume for related to public access protections, refer to ARS Appendix A for e-Authentication Standards. ublic-facing MA to determine if e-authentication is required and implemented in conjunction with or	for e-Authentication Standards. Related Controls: nd procedures; boundary protection procedures; information ents or records to determine if e-authentication is required and r related to public access protections; refer to ARS Appendix A for
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object Examine: System and communic system design documentation; inf implemented in conjunction with content of the information of the Interview: MA owners for each pu e-Authentication Standards.	biblicly accessible systems, as well as the integrity of publicly accessible applications. Moderate) I implemented in conjunction with or related to public access protections, refer to ARS Appendix A i References: ARS: SC-14(CMS-2) C-14(CMS-2).1 em protects the integrity and availability of publicly available information and applications. cts cations protection policy; procedures addressing public access protections; access control policy ar formation system configuration settings and associated documentation; and other relevant docume or related to public access protections, refer to ARS Appendix A for e-Authentication Standards.	for e-Authentication Standards. Related Controls: nd procedures; boundary protection procedures; information ents or records to determine if e-authentication is required and r related to public access protections; refer to ARS Appendix A for
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (N Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object Examine: System and communic system design documentation; inf implemented in conjunction with of Interview: MA owners for each pu e-Authentication Standards. Test: All public-facing systems to Standards.	bilicity accessible systems, as well as the integrity of publicity accessible applications. Moderate) implemented in conjunction with or related to public access protections, refer to ARS Appendix A in References: ARS: SC-14(CMS-2) C-14(CMS-2).1 emprotects the integrity and availability of publicity available information and applications. cts formation system configuration settings and associated documentation; and other relevant docume or related to public access protections, refer to ARS Appendix A for e-Authentication Standards. ublic-facing MA to determine if e-authentication is required and implemented in conjunction with or related to public access protection with or related to public access protection with or related to public access protection with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards. ublic-facing MA to determine if e-authentication is required and implemented in conjunction with or related to public access protections is required and implemented in conjunction with or related to public access protections.	for e-Authentication Standards. Related Controls: nd procedures; boundary protection procedures; information ents or records to determine if e-authentication is required and r related to public access protections; refer to ARS Appendix A for
processed, and transmitted by pu SC-14(CMS-2) – Enhancement (I Control If e-authentication is required and Applicability: All ASSESSMENT PROCEDURE: SC Assessment Objective Determine if the information syste Assessment Methods And Object Examine: System and communic system design documentation; inf implemented in conjunction with c Interview: MA owners for each pu e-Authentication Standards. Test: All public-facing systems to	bilicity accessible systems, as well as the integrity of publicity accessible applications. Moderate) implemented in conjunction with or related to public access protections, refer to ARS Appendix A in References: ARS: SC-14(CMS-2) C-14(CMS-2).1 emprotects the integrity and availability of publicity available information and applications. cts formation system configuration settings and associated documentation; and other relevant docume or related to public access protections, refer to ARS Appendix A for e-Authentication Standards. ublic-facing MA to determine if e-authentication is required and implemented in conjunction with or related to public access protection with or related to public access protection with or related to public access protection with or related to public access protections, refer to ARS Appendix A for e-Authentication Standards. ublic-facing MA to determine if e-authentication is required and implemented in conjunction with or related to public access protections is required and implemented in conjunction with or related to public access protections.	for e-Authentication Standards. Related Controls: nd procedures; boundary protection procedures; information ents or records to determine if e-authentication is required and r related to public access protections; refer to ARS Appendix A for

Guidance		
Collaborative computing mecha microphones are activated.	anisms include, for example, video and audio conferencing capabilities. Explicit indication of use	e includes, for example, signals to local users when cameras and/o
Applicability: All	References: ARS: SC-15; NIST 800-53/53A: SC-15; PISP: 4.16.15	Related Controls:
ASSESSMENT PROCEDURE:	SC-15.1	
Assessment Objective		
Determine if the information sys	stem prohibits remote activation of collaborative computing mechanisms and provides an explic	cit indication of use to the local users.
Assessment Methods And Ob		
Examine: System and commun	nications protection policy; procedures addressing collaborative computing; access control polic	cy and procedures; information system design documentation;
	on settings and associated documentation; other relevant documents or records.	
	implementing access controls for collaborative computing environments; alert notification for lo	cal users.(Optional)
SC-15(1) – Enhancement (Moc	lerate)	
Control		
	nanisms are authorized in writing by the CIO or his/her designated representative:	
Applicability: All	cameras or microphones in a manner that supports ease of use. References: ARS: SC-15(1); NIST 800-53/53A: SC-15(1)	Related Controls:
ASSESSMENT PROCEDURE:		Related Controls.
	50-10(1).1	
Assessment Objective	stem provides physical disconnect of camera and microphone in a manner that supports ease of	ofuso
Assessment Methods And Ob		or use.
	nications protection policy; procedures addressing collaborative computing; access control polic	cy and procedures: information system design documentation:
	on settings and associated documentation; other relevant documents or records.(Optional)	cy and procedures, mormation system design documentation,
	Ilaborative computing devices.(Optional)	
SC-15(CMS-1) - Enhancement		
Control		
	nanisms are authorized in writing by the CIO or his/her designated representative:	
Ensure the information system		
	ceptable use of collaborative computing mechanisms to the local users (e.g., camera or microp	phone), and
	al user of the fact that it is in use.	
Applicability: All	References: ARS: SC-15(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE:	SC-15(CMS-1).1	
Assessment Objective		
-	stem prohibits remote activation of collaborative computing mechanisms and provides an explicit	cit indication of use to the local users.
Assessment Methods And Ob		
	nications protection policy; procedures addressing collaborative computing; access control polic on settings and associated documentation; and other relevant documents or records to determine	
	ceptable use of collaborative computing mechanisms to the local users (e.g., camera or microp	
	al user of the fact that it is in use.	
Interview: Personnel to determ	nine if the information system provides:	
	ceptable use of collaborative computing mechanisms to the local users (e.g., camera or microp	phone), and
	al user of the fact that it is in use.	
	implementing access controls for collaborative computing environments and alert notification for	
	ceptable use of collaborative computing mechanisms to the local users (e.g., camera or microp al user of the fact that it is in use.	none), and
	ecurity Parameters (Moderate)	
	curry rarameters (moderate)	
Control		
Toobpicol controls shall be devi	alanad documented and implemented offectively to answe that CMC information suctions and	ably approximate apprintly parameters with information and a set to the
Technical controls shall be dev	eloped, documented, and implemented effectively to ensure that CMS information systems reli-	ably associate security parameters with information exchanged bet

information systems.		
Guidance		
	ity labels and markings. Security parameters may be explicitly or implicitly associated	
	References: ARS: SC-16; NIST 800-53/53A: SC-16; PISP: 4.16.16	Related Controls:
ASSESSMENT PROCEDURE: SC-16.1		
Assessment Methods And Objects Examine: System and communications protecti	ociates security parameters with information exchanged between information system on policy; procedures addressing transmission of security parameters; access contro	ol policy and procedures; boundary protection procedures;
, .	nation system configuration settings and associated documentation; other relevant d	ocuments of records.(Optional)
11 0	le transmission of security parameters between information systems.(Optional)	
SC-17 – Public Key Infrastructure Certif	icates (moderate)	
key certificate shall include authorization by a succertificate is issued to the intended party.	formation system shall be issued in accordance with a defined certification policy an upervisor or a responsible official, and shall be done by a secure process that verifies	
	shes an agency certification authority cross-certified with the Federal Bridge Certifica equired by OMB Memorandum 05-24. NIST SP 800-32 provides guidance on public l	
Applicability: All	References: ARS: SC-17; NIST 800-53/53A: SC-17; PISP: 4.16.17	Related Controls:
ASSESSMENT PROCEDURE: SC-17.1	•	•
32; other relevant documents or records.	on policy; procedures addressing public key infrastructure certificates; public key cert	tificate policy or policies; public key issuing process; NIST SP 800
ě i i	key infrastructure certificate issuing responsibilities.(Optional)	
SC-18 – Mobile Code (Moderate)		
	ementation guidance for mobile code technologies based on the potential to cause has been use of mobile code within the CMS information system. Appropriate officials shall ode in accordance with NIST SP 800-28.	
apply to both the selection and use of mobile co	Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, ar de installed on organizational servers and mobile code downloaded and executed on cceptable mobile code within the information system. NIST SP 800-28 provides guida	n individual workstations. Control procedures prevent the
Applicability: All	References: ARS: SC-18; NIST 800-53/53A: SC-18; PISP: 4.16.18	Related Controls:
ASSESSMENT PROCEDURE: SC-18.1		
and	s and implementation guidance for mobile code technologies based on the potential ontrols the use of mobile code within the information system.	to cause damage to the information system if used maliciously;
Examine: System and communications protecti	on policy; procedures addressing mobile code; mobile code usage restrictions, mobil	le code implementation guidance; NIST SP 800-28; other relevar
D 0	Daga 166 af 190	DDCCM Annondin A Attachment

o 1	code authorization, monitoring, and control responsibilities.(Optional)	
Test: Mobile code authorization and monitoring c		
SC-19 – Voice Over Internet Protocol (M	oderate)	
	mentation guidance for Voice over Internet Protocol (VoIP) technologies base for the use of VoIP within a CMS information system. When VoIP is impleme	
Guidance	anaidarationa for ValD technologiae ampleued in information austama	
	considerations for VoIP technologies employed in information systems. References: ARS: SC-19; NIST 800-53/53A: SC-19; PISP: 4.16.19	Related Controls:
ASSESSMENT PROCEDURE: SC-19.1	References: AR3. 30-19, NI31 800-35/35A. 30-19, FISF. 4.10.19	Related Controls.
maliciously; and (ii) the organization authorizes, monitors, and cor Assessment Methods And Objects Examine: System and communications protectio	s and implementation guidance for Voice over Internet Protocol technologies b ntrols the use of VoIP within the information system. on policy; procedures addressing VoIP; NIST SP 800-58; VoIP usage restrictio	
	uthorization and monitoring responsibilities.(Optional)	
SC-19(CMS-1) – Enhancement (Moderate)		
Control	the CMS CIO, or his/her designated representative.	
	References: ARS: SC-19(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SC-19(CMS-1).		Inclated Controls.
maliciously; and (ii) the organization authorizes, monitors, and cor	s and implementation guidance for Voice over Internet Protocol technologies b ntrols the use of VoIP within the information system.	based on the potential to cause damage to the information system if used
Assessment Methods And Objects	an policy around trace addressing ValD: NICT CD 200 59: ValD upage restriction	and other relevant desumants or records to determine if the use of
VoIP is authorized in writing by the CMS CIO, or Interview: Organizational personnel with VoIP au	uthorization and monitoring responsibilities to determine if the information syst ollaborative computing mechanisms to the local users (e.g., camera or microph	tem provides:
SC-20 – Secure Name / Address Resolut	tion Service (Authoritative Source) (Moderate)	
Control		
Technical controls shall be developed, document	ted, and implemented effectively to ensure that each information system that p ritative data it returns in response to resolution queries.	provides name / address resolution service provides additional data
Guidance		
This control enables remote clients to obtain origi system (DNS) server is an example of an informa resource records are examples of authoritative da	in authentication and integrity verification assurances for the name/address re ation system that provides name/address resolution service; digital signatures ata. NIST SP 800-81 provides guidance on secure domain name system deplo	and cryptographic keys are examples of additional artifacts; and DNS
	References: ARS: SC-20; NIST 800-53/53A: SC-20; PISP: 4.16.20	Related Controls:
ASSESSMENT PROCEDURE: SC-20.1		
Assessment Objective		
Determine if the information system that provides	s the name/address lookup service for accessing organizational information re-	sources to entities across the Internet provides artifacts for additional

data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.

Assessment Methous And Objects		
	tion policy; procedures addressing secure name/address resolution service (authoritativ	ve source); NIST SP 800-81; information system design
	on settings and associated documentation; other relevant documents or records.	tom (Ontional)
	ecure name/address resolution service (authoritative source) within the information syst	tem.(Optional)
· · · · · · · · · · · · · · · · · · ·	for Name / Address Resolution Service (Moderate)	
Control		
, , , , , , , , , , , , , , , , , , ,	ame / address resolution service for an organization shall be fault tolerant and impleme	ent role separation.
Guidance		
are typically at least two authoritative domain n network subnets and geographically separated networks and those resources belonging to ext name/address resolution information pertaining information pertaining to external information te guidance on secure DNS deployment.	ample of an information system that provides name/address resolution service. To elimi name system (DNS) servers, one configured as primary and the other as secondary. Ad I (i.e., not located in the same physical facility). If organizational information technology ternal networks, authoritative DNS servers with two roles (internal and external) are esta g to both internal and external information technology resources while the DNS server w echnology resources. The list of clients who can access the authoritative DNS server of	dditionally, the two servers are commonly located in two different resources are divided into those resources belonging to internal tablished. The DNS server with the internal role provides with the external role only provides name/address resolution
Applicability: All	References: ARS: SC-22; NIST 800-53/53A: SC-22; PISP: 4.16.22	Related Controls:
ASSESSMENT PROCEDURE: SC-22.1		
Assessment Methods And Objects	ctively provide name/address resolution service for an organization are fault tolerant an	
800-81; information system design documentative relevant documents or records.	tion policy; procedures addressing architecture and provisioning for name/address reso tion; assessment results from independent, testing organizations; information system co e/address resolution service for fault tolerance and role separation.(Optional)	
SC-23 – Session Authenticity (Modera	te)	
Control		
Technical controls shall be developed, docume	ented, and effectively implemented to ensure that CMS information systems provide me	echanisms to protect the authenticity of communications sessions.
Guidance		
architectures providing web-based services). N	ction at the session, versus packet, level. The intent of this control is to implement sessi NST SP 800-52 provides guidance on the use of transport layer security (TLS) mechani er methods of protecting communications sessions. NIST SP 800-95 provides guidance	isms. NIST SP 800-77 provides guidance on the deployment of
Applicability: All	References: ARS: SC-23; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: SC-23; PISP: 4	
ASSESSMENT PROCEDURE: SC-23.1		
Assessment Objective		
Determine if the information system provides m	nechanisms to protect the authenticity of communications sessions.	
Assessment Methods And Objects		
	tion policy; procedures addressing session authenticity; NIST SP 800-52, 800-77, and 8 documentation; other relevant documents or records.	800-95; information system design documentation; information
SC-CMS-1 – Desktop Modems (Modera		
Control		
Users are prohibited from installing desktop mo	odems	
Guidance	20010.	
Desktop Modems allow backdoors into the net	work putting the CMS data and network at very high risk	
Desktop Modems allow backdoors into the netw Applicability: All	work putting the CMS data and network at very high risk. References: ARS: SC-CMS-1; PISP: 4.16.24	Related Controls:

Assessment Methods And Objects

Determine it fine organization has implement a policy which assists in prohibiting the installation of unauthorized deskop modems. Sec-CMS-2 - Identify and Detect Unauthorized deskop modems. Sec-CMS-2 - Identify and Detect Unauthorized Modems (Moderate) Control Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized modems. Suidance It is good practice that management approve any automated tool or utily for checking for unauthorized modems. Suidance It is good practice that management approve any automated tool or utily for checking for unauthorized modems. Suidance It is good practice that management approve any automated tool or utily for checking for unauthorized modems. Sessessment Objective Determine if the organization has an approved automated system to test for unauthorized modems. Sessessment Deforms a completer review no less than quarterly. It for organization has an approved automated system to test for unauthorized modems. Sessessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a completer review no less than quarterly. Sec CMS-2/CMS-0/ = Enhancement (Moderate) Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a completer review no less than quarterly. Sec CMS-2/CMS-0/ = Enhancement (Moderate) Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Sessessment Objective Determine if t	ASSESSMENT PROCEDURE: SC-CMS-1.1		
Assessment Methods And Objects Image: Comparison of policy does not allow unauthorized desktop moders. Sci-CMS-2 - Identify and Detect Unauthorized Moderns (Moderate) Image: Comparison of policy does not allow unauthorized Moderns. Suidance It is good practice that management approve any automated tool or utility for checking for unauthorized moders. Spatiations / Display and Detect Unauthorized Moderns / RS: SC-CMS-2, PISP: 4.16.25 Related Controls: SSSESSMENT PROCEDURE: SC-CMS-2.1 Secondary (State and State	Assessment Objective		
Examine: Organizational policy does not allow unauthorized desktop modems. SC-CMS-2 - Identify and Detect Unauthorized Modems (Moderate) Control Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized modems. SUdiance It is good practice that management approve any automated tool or utility for checking for unauthorized modems. References: ARS: SC-CMS-2, PSP-4.16.25 References: ARS: SC-CMS-2, PSP-4.16.25 References: ARS: SC-CMS-2, PSP-4.16.25 References: ARS: SC-CMS-2, PSP-4.16.25 ASSESSMENT PROCEDURE: SC-CMS-2.1 Assessment Objective Determine if the organization has an approved automated system to test for unauthorized modems. Assessment Deforms a completer review no less than quarterly. Interview: Organization has an approved automated system to test for unauthorized modems. SeeSSMENT PROCEDURE: SC-CMS-2.1 References: RS: SC-CMS-2, PSP-4.16.25 Research of the organization has an approved automated system to test for unauthorized modems. SeeSSMENT Deforms a completer review no less than quarterly. Interview: Organization approved automated systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a completer review no less than quarterly. See CMS-2 (CMS-0) = Enhancement (Moderate) Control Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a completer review no less than quarterly. See See Set SCMS-2 (CMS-0) = References: RS: SC-CMS-2 (CMS-0) References: RS: SC-CMS-2 (CMS-0	5 1 1	olicy which assists in prohibiting the installation of unauthorized desktop mo-	dems.
SC-CMS-2 – Identify and Detect Unauthorized Moders (Moderate) Control Advanated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized moderns. Is good bacice that management approve any automated tool or utility for checking for unauthorized moderns. Is good bacice that management approve any automated tool or utility for checking for unauthorized moderns. References: ARS. SC-CMS-2; PISP: 4.16.25 Research Objective Determine if the organization has an approved automated system to test for unauthorized moderns. Research Objective Determine if the organization provide automated system to test for unauthorized moderns. Research Researc			
Control Automated methods and related procedures shall be established, documented and implemented effectively to identify and detect unauthorized modems. Biglicability: All References: ARS: SC:CMS-2; PISP: 4.16.25 Related Controls: Related Controls: ASSESSMENT PROCEDURE: SC-CMS-2.1 Reservences: Reservences: ARS: SC:CMS-2; PISP: 4.16.25 Related Controls: Reservence: ARS: SC:CMS-2;			
Automated methods and related procedures shall be established, documented and implemented effectively to identify and deted unauthorized modems. Bit is good practice that management approve any automated tool or utility for checking for unauthorized modems. Related Controls: SSESSMENT PROCEDURE; SC-CMS-2.1 Related Controls: SSESSment Buthods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. Related Controls: SSESSMENT PROCEDURE; SC-CMS-2.1 Related Controls: Constraints Related controls: Sassessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Constraint References: ARS: SC-CMS-2(CMS-0) Related Controls: SSESSMENT PROCEDURE; SC-CMS-2(CMS-0).1 Reserve References: ARS: SC-CMS-2(CMS-0) Related Controls: SSESSMENT PROCEDURE; SC-CMS-2(CMS-0).1 References: ARS: SC-CMS-2(CMS-0) Related Controls: References: ARS: SC-CMS-2(CMS-0) Related Controls:	SC-CMS-2 – Identify and Detect Unauth	orized Modems (Moderate)	
Guidance It is god practice that management approve any automated tool or utility for checking for unauthorized moderns. Assessment Objective References: ARS: SC-CMS-2; PISP: 4.16.25 Assessment Objective Reterences: ARS: SC-CMS-2; PISP: 4.16.25 Assessment Objective Reterences: ARS: SC-CMS-2; PISP: 4.16.25 Assessment Objective Reterences: ARS: SC-CMS-2; PISP: 4.16.25 Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational performs a complete review no less than quarterly. Reterences: ARS: SC-CMS-2(CMS-0) Scottrol Reterences: ARS: SC-CMS-2(CMS-0) Reterences: ARS: SC-CMS-2(CMS-0) Sessessment Nethods And Objects References: ARS: SC-CMS-2(CMS-0) Reterences: ARS: SC-CMS-2(CMS-0) Sessessment Objective Reterences: ARS: SC-CMS-2(CMS-0) Reterences: ARS: SC-CMS-2(CMS-0) Sessessment Objective Reterences: ARS: SC-CMS-2(CMS-0) Retained controls: Sessessment Objective Reterences: ARS: SC-CMS-2(CMS-0) Retaine control. Sessessment Objective Reterences: ARS: SC-CMS-2(CMS-0) Retaine control. Sessessment Objective Determine if network systems use an automated method to de	Control		
It is good practice that management approve any automated tool or utility for checking for unauthorized moderns. Releted Controls: ASSESSMENT PROCEDURE: SC-CMS-2.1 Releted Controls: ASSESSMENT PROCEDURE: SC-CMS-2.1 Releted Controls: Assessment Objective Determine if the organization has an approved automated system to test for unauthorized moderns. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization parforms a complete review no less than quarterly. Interview: Organizational performs a complete review no less than quarterly. Seconds 20(CMS-0) ColMS-20(CMS-0) References: ARS: SC-CMS-2(CMS-0) Related Controls: Assessment Objective References: ARS: SC-CMS-3(CMS-0) Related Controls:	Automated methods and related procedures sha	all be established, documented and implemented effectively to identify and de	etect unauthorized modems.
Applicability: All References: ARS: SC-CMS-2; PISP: 4.16.25 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-2.1 ASSESSMENT PROCEDURE: SC-CMS-2.1 ASSESSMENT PROCEDURE: SC-CMS-2.1 Assessment Objective Determine if the organization has an approved automated system to test for unauthorized moderns. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review to less than quarterly. Interview: Organization applice roview to less than quarterly. Sc-CMS-2(CMS-0) = Enhancement (Moderate) Control References: ARS: SC-CMS-2(CMS-0) Related Controls: ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1 Relerences: ARS: SC-CMS-2(CMS-0) Related Controls: Assessment Objective Determine if the organization meets the requirements a specified in the	Guidance		
ASSESSMENT PROCEDURE: SC-CMS-2.1 Assessment Objective Determine if the organization has an approved automated system to test for unauthorized moderns. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. Sc-CMS-2(CMS-0) = Enhancement (Moderate) Control Examine: a sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Sc-CMS-2(CMS-0) = Enhancement (Moderate) Control Examine is a sample of network systems on demand using an automated method to determine if unauthorized moderns are present. Perform a complete review no less than quarterly. Applicability: All References: ARS: SC-CMS-2(CMS-0) Related Controls: Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Network documentemine in flextwork systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Network documentemine in flextwork systems are an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Netw			
Assessment Objective Determine if the organization has an approved automated system to test for unauthorized moderns. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Second Se		References: ARS: SC-CMS-2; PISP: 4.16.25	Related Controls:
Determine if the organization has an approved automated system to test for unauthorized modems. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. CocCMS*2C(CMS+0) = Enhancement (Moderate) Control Examine: a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly. Applicability: All References: ARS: SC-CMS-2(CMS-0) Assessment Objective Related Controls: Assessment Objective Determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization mets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Nethods And Objective Determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to det	ASSESSMENT PROCEDURE: SC-CMS-2.1		
Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. SC-CMS-2(CMS-0) Enhancement (Moderate) Control Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly. Applicability: All References: ARS: SC-CMS-2(CMS-0) Related Controls: ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0,1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than	Assessment Objective		
Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. SC-CMS-2(CMS-0) = Enhancement (Moderate) Control Examine: a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly. Applicability: All References: ARS: SC-CMS-2(CMS-0) Resessment Objective Related Controls: Assessment Objective Related Controls: Resessment Objective Determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Wethods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization appension a complete review no less than quarterly. The available on demand and the organization performs are complete review no less than quarterly. Reservert Retated Controls: Secondary Authentication and Encryption (Moderate) Control Appropriate tech		automated system to test for unauthorized modems.	
arganization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. SC-CMS-2(CMS-0) = Enhancement (Moderate) Control Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly. SSESSMENT PROCEDURE: SC-CMS-2(CMS-0). Related Controls: ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0). Seessment Objective Determine if the organization metrix the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Reseasement Objective Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network systems and and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network. SSESSEMENT PROCEDURE: SC-CMS-3.1 SESSEMENT PROCEDURE: SC-CMS-3.1 SE	Assessment Methods And Objects		
Interview: Organization personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. SC-CMS-2(CMS-0) - Enhancement (Moderate) References: ARS: SC-CMS-2(CMS-0) Related Controls: SSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1 Research Research Research Assessment Objective Determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. References: ARS: SC-CMS-2(CMS-0) Related Controls: SSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1 Assessment Methods And Objects Related Controls: Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. References: Assame the theorem and the theorem and the theorem and the theorem and performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. References: Assame theorem and quarterly. SC-CMS-3 - Secondary Authentication and Encryption (Moderate) References: Ass			etwork services (e.g., modems, etc.) are available on demand and the
organization performs a complete review no less than quarterly. SC-CMS-2(CMS-0) — Enhancement (Moderate) Control Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly. Applicability: All References: ARS: SC-CMS-2(CMS-0) References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; FISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-31 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects			
SC-CMS-2(CMS-0) – Enhancement (Moderate) Control Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly. Applicability: All References: ARS: SC-CMS-2(CMS-0) Related Controls: ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Objective Determine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs to determine in tetwork systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects			network services (e.g., modems, etc.) are available on demand and the
Control Examine a sample of network systems on demand using an automated method to determine if unauthorized moderns are present. Perform a complete review no less than quarterly. References: ARS: SC-CMS-2(CMS-0) Related Controls: ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., moderns, etc.) are available on demand and the organization performs a complete review no less than quarterly. Sc-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handing sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Dejective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-tran			
Examine a sample of network systems on demand using an automated method to determine if unauthorized modems are present. Perform a complete review no less than quarterly. Applicability: All References: ARS: SC-CMS-2(CMS-0) Assessment Objective Related Controls: Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. Interview: a sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for han			
Applicability: All References: ARS: SC-CMS-2(CMS-0) ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less than quarterly. Control Agpropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Resessment Objective References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 <td></td> <td>and using an automated method to determine if unauthorized moderns are pre-</td> <td>poont. Porform a complete review no loss than quarterly</td>		and using an automated method to determine if unauthorized moderns are pre-	poont. Porform a complete review no loss than quarterly
ASSESSMENT PROCEDURE: SC-CMS-2(CMS-0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects			
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Objective			Related Controls.
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects			
Assessment Methods And Objects Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	·····	mente as aposified in the baseline central and the aposifie CMS requirements	as prescribed in this amplifying appendement to the baseline control
Examine: Network documentation to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Interview: Organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secure network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects And Objects Science of the organization has policies in place to provide technical controls to protect sensitive data in-transit.	o 1	There's as specified in the baseline control and the specific CMS requirements	as prescribed in this amplifying enhancement to the baseline control.
organization performs a complete review no less than quarterly. Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects		if network systems use an automated method to determine if unnecessary n	atwork services (e.g. modems, etc.) are available on demand and the
Interview: Organizational personnel to determine if network systems use an automated method to determine if unnecessary network services (e.g., modems, etc.) are available on demand and the organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less than quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects			etwork services (e.g., moderns, etc.) are available on demand and the
organization performs a complete review no less than quarterly. Test: A sample of network systems on demand using an automated method to determine if unnecessary network services (e.g., modems, etc.) are available. Perform a complete review no less tha quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects			network services (e.g., modems, etc.) are available on demand and the
quarterly. SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects			
SC-CMS-3 – Secondary Authentication and Encryption (Moderate) Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	Test: A sample of network systems on demand	using an automated method to determine if unnecessary network services (e	.g., modems, etc.) are available. Perform a complete review no less that
Control Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	quarterly.		
Appropriate technical controls shall be developed, documented, and implemented effectively to assure the identity of users and protect the in-transit confidentiality of their sessions outside the secur network.	SC-CMS-3 – Secondary Authentication	and Encryption (Moderate)	
network. Guidance A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	Control		
A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects		d, documented, and implemented effectively to assure the identity of users a	nd protect the in-transit confidentiality of their sessions outside the secure
A good place to obtain technical controls for handling sensitive information in-transit is the NIST SP. Applicability: All References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 Related Controls: ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	Guidance		
ASSESSMENT PROCEDURE: SC-CMS-3.1 Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	A good place to obtain technical controls for har	Idling sensitive information in-transit is the NIST SP.	
Assessment Objective Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	Applicability: All	References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26	Related Controls:
Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	ASSESSMENT PROCEDURE: SC-CMS-3.1		
Determine if the organization has policies in place to provide technical controls to protect sensitive data in-transit. Assessment Methods And Objects	Assessment Objective		
Assessment Methods And Objects	•	ce to provide technical controls to protect sensitive data in-transit.	
	-	it and documents for sensitive information outside the secure network.	

SC-CMS-3(CMS-0) – Enhancement (Moderate)	
Control	
Enable application security mechanisms, such as Transport Layer Security (TLS). Utilize CMS-approved encryption and password auther	stigation mathada
Applicability: All References: ARS: SC-CMS-3(CMS-0)	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-3(CMS-0).1	Related Controls.
Assessment Objective	d for this second to the second sector that the second sector the
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed	a in this amplifying enhancement to the baseline control.
Assessment Methods And Objects	on a start in a still and on the second start in a start
Examine: Documentation to determine if the organization enables and forces use of application security mechanisms, such as TLS. The password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based authentication or additional authentication protection (e.g., token-based authentication or additional authentication protection (e.g., token-based authentication authentication protection (e.g., token-based authentication authentication protection (e.g., token-based authentication authentication authentication protection (e.g., token-based authentication authentication authentication protection (e.g., token-based authentication	
Interview: Organizational personnel to determine if the organization enables and forces use of application security mechanisms, such as	
and password authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., tok	ken-based, biometric).
Test: Information system to determine if the organization enables and forces use of application security mechanisms, such as TLS. The organization enables and forces use of application security mechanisms, such as TLS.	
authentication methods, in combination with certificate-based authentication or additional authentication protection (e.g., token-based, bior	
SC-CMS-3(CMS-1) – Enhancement (Moderate)	
Control	
If e-authentication is required and implemented, refer to ARS Appendix A for e-Authentication Standards controls and procedures.	
Applicability: All References: ARS: SC-CMS-3(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-3(CMS-1).1	
Assessment Objective	
Determine if the organization that uses e-authentication is required to refer to ARS Appendix A for e-Authentication Standards controls and	d procedures.
Assessment Methods And Objects	
Examine: Network documentation to determine which recommends enabling application security mechanisms, such as TLS, and utilizing	minimum encryption and password authentication although,
no specific requirements are mandatory.	
Interview: Organizational personnel to determine if enabling application security mechanisms is recommended, such as TLS, and utilizing	minimum encryption and password authentication although,
no specific requirements are mandatory.	
Test: Information system to determine if application security mechanisms are enabled, such as TLS, and the organization utilizes minimum	n encryption and password authentication although, no
specific requirements are mandatory.	
SC-CMS-4 – Electronic Mail (Moderate)	
Control	
Controls shall be developed, documented, and implemented effectively to protect CMS sensitive information that is sent via e-mail.	
Guidance	
A good place to obtain technical controls for handling sensitive information via e-mail is the NIST SP.	
Applicability: All References: ARS: SC-CMS-4; PISP: 4.16.27	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-4.1	
Assessment Objective	
Determine if the organization effectively develops, documents, and implements protections for CMS sensitive information that is sent via e	-mail.
Assessment Methods And Objects	
Examine: Documentation to determine if all e-mail messages with CMS sensitive information are transmitted using protective measures.	
Interview: Organizational personnel to determine if all e-mail messages with CMS sensitive information is protected, controlled, and monitorial controlled and controlled and monitorial controlled and monitorial controlled and monitorial controlled and cont	itored.
SC-CMS-4(CMS-0) – Enhancement (Moderate)	
Control	
Prior to sending an email, place all CMS sensitive information in an encrypted attachment.	
Applicability: All References: ARS: SC-CMS-4(CMS-0); IRS-1075: 5.7.3#1	Related Controls:

ASSESSMENT PROCEDURE: SC-CMS-4(CMS-0).1	
Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ing ophonooment to the baseline control
Assessment Methods And Objects	ang enhancement to the baseline control.
Examine: Documentation to determine if all e-mail messages are encrypted and verify encryption / decryption for received messages.	
Interview: Organizational personnel to determine if all e-mail messages are encrypted and verify encryption /decryption for received messages.	
SC-CMS-5 – Persistent Cookies (Moderate)	
Control	
The use of persistent cookies on a CMS web site is prohibited unless explicitly approved in writing by the DHHS Secretary.	
Guidance	
Requests to DHHS should be via CMS.	
Applicability: All References: ARS: SC-CMS-5; PISP: 4.16.28	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-5.1	•
Assessment Objective	
Determine if the organization does not use a persistent cookie configuration on a CMS web site to remember subsequent visits unless approved in writin	g by the DHHS Secretary.
Assessment Methods And Objects	
Examine: CMS web site baseline and change management documentation for configurations using persistent cookies.	
Interview: Web site administrators to determine if the CMS web site has persistent cookies enable in the baseline configuration or have written approval	to enable persistent cookies from the DHHS
Secretary.	
SC-CMS-6 – Network Interconnection (Moderate)	
Control	
Controls shall be developed, documented, and implemented effectively to ensure that only properly authorized network interconnections external to the	system boundaries are established.
Guidance	
A good place to obtain technical controls for securing interconnections external to the system boundaries is the NIST SP.	
Applicability: All References: ARS: SC-CMS-6; PISP: 4.16.29	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-6.1	
Assessment Objective	
Determine if the organization effectively documents and implements authorized network interconnections external to the system boundaries.	
Assessment Methods And Objects	
Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards for all external interconnections.	
SC-CMS-6(CMS-0) – Enhancement (Moderate)	
Control	
Ensure remote location(s) (e.g., users and sites using a network interconnection external to the system boundaries) follow all CMS IS policies and stand	ards and obtain a signed interconnection
Security Agreement. Desument the interconnection in the SSD for the system that is connected to the remote location	
Security Agreement. Document the interconnection in the SSP for the system that is connected to the remote location. Applicability: All References: ABS: SC-CMS-6(CMS-0): FISCAM: TAC-2.1.3, TAC-2.3.2	-
Applicability: All References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2	Related Controls:
Applicability: All References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2 ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1	-
Applicability: All References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2 ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1 Assessment Objective	Related Controls:
Applicability: All References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2 ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplified in the baseline control and the specific CMS requirements as prescribed in this amplified in the baseline control and the specific CMS requirements as prescribed in this amplified in the baseline control and the specific CMS requirements as prescribed in this amplified in the baseline control and the specific CMS requirements as prescribed in the	Related Controls:
Applicability: All References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2 ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplif Assessment Methods And Objects	Related Controls:
Applicability: All References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2 ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplif Assessment Methods And Objects Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreen SSP for the system that is connected to the remote location.	Related Controls:
Applicability: All References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2 ASSESSMENT PROCEDURE: SC-CMS-6(CMS-0).1 Assessment Objective Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplif Assessment Methods And Objects Examine: Documentation to determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Security Agreem	Related Controls:

System and Information Integrity (SI) – Operational

SI-1 – System and Information Integrity Policy and Procedures (Moderate)

Control

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems, software, and information. The procedures and automated mechanisms shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. It is good practice to have an automated system which is host based to automatically detect, block/filter and alert supervisors or managers that possible unauthorized changes to software and the information system have occurred.

Applicability: All	References: AR PISP: 4.17.1	S: SI-1; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2;	NIST 800-53/53A: SI-1;	elated Controls:

ASSESSMENT PROCEDURE: SI-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents system and information integrity policy and procedures;

(ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and information integrity policy and procedures; and

(iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and information integrity responsibilities.(Optional)

ASSESSMENT PROCEDURE: SI-1.2

Assessment Objective

Determine if:

(i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with system and information integrity responsibilities.(Optional)

SI-2 – Flaw Remediation (Moderate)

Control

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. The flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

Guidance

The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. It is a good practice to test the changes in a laboratory environment on like systems prior to approving and implementing the updates and changes. NIST SP 800-40, provides guidance on security patch installation and patch management.

Applicability: All References: ARS: SI-2; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST & PISP: 4.17.2	800-53/53A: SI-2; Related Controls: CA-2, CA-4, CA-7, CM- 3, IR-4, SI-11
---	---

ASSESSMENT PROCEDURE: SI-2.1

Assessment Objective

Determine if:

(i) the organization identifies, reports, and corrects information system flaws;

(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;

(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures;

(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and

(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(0) – Enhancement (Moderate)

Control

Correct identified information system flaws on production equipment within one (1) week.

(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and

(b) Manage the flaw remediation process centrally.

Applicability: All	References: ARS: SI-2(0); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2;	Related Controls:
	PISP: 4.17.2	

ASSESSMENT PROCEDURE: SI-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.

SI-2(1) – Enhancement (Moderate)

Control

Updates are installed automatically.

Applicability: All	References: ARS: SI-2(1); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2	Related Controls:
ASSESSMENT PROCEDURE: SI-2(1).1		

Assessment Objective

Determine if the organization centrally manages the flaw remediation process and installs updates automatically.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records.(Optional)

Test: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates.(Optional)

SI-2(2) – Enhancement (Moderate)	SI-2(2) – Enhancement (Moderate)		
Control	Control		
Employ automated mechanisms periodically and upon demand to determine the state of information system components with regard to flaw remediation.			
	Potoroncos: APS: SI 2(2): HIPAA: 164 209(2)(1)(i): IPS 1075: 5.6.2.5#1.1.2: NIST 200.52/53A: SI	Polated Controls:	

Applicability: All	References: ARS: SI-2(2); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-	Related Controls:
	2(2)	

ASSESSMENT PROCEDURE: SI-2(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation. Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing information system flaw remediation update status.

SI-3 – Malicious Code Protection (Moderate)

Control

Automated malicious code protection mechanisms that include a capability of automatic updates shall be in place and supporting procedures shall be developed, documented, and implemented effectively to identify and isolate suspected malicious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical information system entry points, and at each workstation, server, or mobile computing device on the network to detect and eradicate malicious code transported by email, email attachments, removable media or other methods. Business owners shall use antiviral software products from multiple vendors, if possible, and update virus protection mechanisms whenever new releases are available.

Guidance

The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization also considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and the resulting potential impact on the availability of the information system. NIST SP 800-83 provides guidance on implementing malicious code protection.

3		
Applicability: All	References: ARS: SI-3; FISCAM: TCC-1.3.2; IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP:	Related Controls:
	4.17.3	

ASSESSMENT PROCEDURE: SI-3.1

Assessment Objective

Determine if:

(i) the information system implements malicious code protection;

(ii) the organization employs malicious code protection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;

(iii) the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities;

(iv) the organization updates malicious code protection mechanisms whenever new releases are available; and

(v) the malicious code protection mechanisms are appropriately updated to include the latest malicious code definitions, configured to perform periodic scans of the information system as well as realtime scans of files from external sources as the files are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(0) – Enhancement (Moderate)

Control

Implement malicious code protection at information system entry points, including firewalls, email servers, remote access servers, workstations, servers, and mobile computing devices by employing automated mechanisms to detect and eradicate malicious code transported by email, email attachments, and removable media.

Applicability: All	References: ARS: SI-3(0); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	Related Controls:
ASSESSMENT PROCEDURE: SI-3(0).1		

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection

	tings and associated documentation; other relevant documents or records.	
SI-3(1) – Enhancement (Moderate)		
Control		
	n software centrally with automatic updates for the latest malicious code definitions when	
Applicability: All	References: ARS: SI-3(1); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3(1)	Related Controls:
ASSESSMENT PROCEDURE: SI-3(1).1		
Assessment Objective		
Determine if the organization centrally manag	es malicious code protection mechanisms.	
Assessment Methods And Objects		
	plicy; procedures addressing malicious code protection; information system design docu	
	n system configuration settings and associated documentation; other relevant documen	its or records.
SI-3(2) – Enhancement (Moderate)		
Control		
Employ automated mechanisms to update ma		Delete d Oenstrade
	References: ARS: SI-3(2); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3(2)	Related Controls:
ASSESSMENT PROCEDURE: SI-3(2).1		
Assessment Objective		
	odates malicious code protection mechanisms.	
Assessment Methods And Objects		
	plicy; procedures addressing malicious code protection; information system design docu n system configuration settings and associated documentation; other relevant documen	
Test: Automatic update capability for maliciou		its of records.
SI-3(CMS-1) – Enhancement (Moderate)		
Control		
	cious code scanning software must be installed, real-time protection and monitoring mus	st be enabled, and the software must be configured to perform
critical system file scans during system boot a		st be chabled, and the software must be comigured to perform
Applicability: All	References: ARS: SI-3(CMS-1); IRS-1075: 5.6.2.5#1.3	Related Controls:
ASSESSMENT PROCEDURE: SI-3(CMS-1)	.1	
Assessment Objective		
Determine if:		
(i) real-time file scanning is enabled;		
(ii) real-time desktop malicious code scanning		
	ystem file scans during system boot and every twenty-four (24) hours.	
Assessment Methods And Objects		
	plicy; procedures addressing malicious code protection; NIST SP 800-83; malicious code	
updates; information system configuration settings and associated documentation; other relevant documents or records to determine real-time file scanning is enabled. Desktop malicious code scanning software must be installed, real-time protection and monitoring must be enabled, and the software must be configured to perform critical system file scans during system boot and every		
twenty-four (24) hours.	protection and monitoring must be enabled, and the software must be configured to pe	anorm critical system file scans during system boot and every
	ation integrity responsibilities to determine real-time file scanning is enabled, desktop m	nalicious code scanning software is installed real-time protection
	s configured to perform critical system file scans during system boot and every twenty-for	
Test: Information system real-time file scanni	ng is enabled, desktop malicious code scanning software is installed, real-time protection	
perform critical system file scans during system boot and every twenty-four (24) hours.		
SI-4 – Information System Monitoring	Tools and Techniques (Moderate)	
Control		
Effective monitoring tools and techniques pro-	viding real-time identification of unauthorized use, misuse, and abuse of the information	system shall be implemented.
Enective monitoring tools and techniques pro	nuing real-time identification of unauthorized use, misuse, and abuse of the information	i system shall be implemented.

Guidance

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information, or other credible sources of information. NIST SP 800-61 provides guidance on detecting attacks through various types of security technologies. NIST SP 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST SP 800-92 provides guidance on monitoring and analyzing computer security event logs.

Applicability: All	References: ARS: SI-4; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4; PISP: 4.17.4	Related Controls: AC-8, AU-4, CM-6
ASSESSMENT PROCEDURE:		1
Assessment Objective		
Determine if the organization e	employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of una	uthorized use of the system.
Assessment Methods And Ob	bjects	
	ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig	
	es documentation; information system configuration settings and associated documentation; other relevant documents or re	ecords.
SI-4(1) – Enhancement (Mode	rate)	
Control		
Connect individual IDS devices	s to a common IDS management network using common protocols.	
Applicability: All	References: ARS: SI-4(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(1)	Related Controls:
ASSESSMENT PROCEDURE:	SI-4(1).1	
Assessment Objective		
Assessment Objective		
	nterconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using commo	on protocols.
Determine if the organization ir	nterconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using commo	on protocols.
Determine if the organization ir Assessment Methods And Ob	pjects	
Determine if the organization ir Assessment Methods And Ob Examine: System and informa		n documentation; information system
Determine if the organization ir Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional)	ojects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols;	n documentation; information system
Determine if the organization ir Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide	ojects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; e intrusion detection capability.(Optional)	n documentation; information system
Determine if the organization ir Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional)	ojects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; e intrusion detection capability.(Optional)	n documentation; information system
Determine if the organization ir Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide	ojects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; e intrusion detection capability.(Optional)	n documentation; information system
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Model Control	ojects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; e intrusion detection capability.(Optional)	n documentation; information system
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Model Control	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; intrusion detection capability.(Optional) rate)	n documentation; information system
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Model Control Monitor inbound and outbound Guidance	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; intrusion detection capability.(Optional) rate)	n documentation; information system other relevant documents or
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Model Control Monitor inbound and outbound Guidance	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system designed documentation; information system protocols; a intrusion detection capability.(Optional) rate) d communications for unusual or unauthorized activities or conditions.	n documentation; information system other relevant documents or
Determine if the organization ir Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Moder Control Monitor inbound and outbound Guidance Unusual/unauthorized activities	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; atintrusion detection capability.(Optional) rate) d communications for unusual or unauthorized activities or conditions. s or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4)	n documentation; information system other relevant documents or
Determine if the organization ir Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Mode Control Monitor inbound and outbound Guidance Unusual/unauthorized activities Applicability: All ASSESSMENT PROCEDURE:	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; atintrusion detection capability.(Optional) rate) d communications for unusual or unauthorized activities or conditions. s or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4)	n documentation; information system other relevant documents or
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Mode Control Monitor inbound and outbound Guidance Unusual/unauthorized activities Applicability: All ASSESSMENT PROCEDURE: Assessment Objective	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; atintrusion detection capability.(Optional) rate) d communications for unusual or unauthorized activities or conditions. s or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4)	n documentation; information system other relevant documents or
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Mode Control Monitor inbound and outbound Guidance Unusual/unauthorized activities Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if:	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; atintrusion detection capability.(Optional) rate) d communications for unusual or unauthorized activities or conditions. s or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4)	n documentation; information system other relevant documents or
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Mode Control Monitor inbound and outbound Guidance Unusual/unauthorized activities Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization identifies th	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; a intrusion detection capability.(Optional) rate) I communications for unusual or unauthorized activities or conditions. s or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4) SI-4(4).1	n documentation; information system other relevant documents or
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Mode Control Monitor inbound and outbound Guidance Unusual/unauthorized activities Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization identifies th	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; a intrusion detection capability.(Optional) rate) I communications for unusual or unauthorized activities or conditions. s or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4) SI-4(4).1 he types of activities or conditions considered unusual or unauthorized; and hitors inbound and outbound communications for unusual or unauthorized activities or conditions.	n documentation; information system other relevant documents or
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Mode Control Monitor inbound and outbound Guidance Unusual/unauthorized activities Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization identifies th (ii) the information system mon Assessment Methods And Ob	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; intrusion detection capability.(Optional) rate) I communications for unusual or unauthorized activities or conditions. s or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4) SI-4(4).1 he types of activities or conditions considered unusual or unauthorized; and hitors inbound and outbound communications for unusual or unauthorized activities or conditions. jects	n documentation; information system other relevant documents or o an external information system. Related Controls:
Determine if the organization in Assessment Methods And Ob Examine: System and informa monitoring tools and technique records.(Optional) Test: Information system-wide SI-4(4) – Enhancement (Mode Control Monitor inbound and outbound Guidance Unusual/unauthorized activities Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization identifies th (ii) the information system mon Assessment Methods And Ob Examine: System and informa	bjects ation integrity policy; procedures addressing information system monitoring tools and techniques; information system desig as documentation; information system configuration settings and associated documentation; information system protocols; a intrusion detection capability.(Optional) rate) I communications for unusual or unauthorized activities or conditions. s or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to References: ARS: SI-4(4); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(4) SI-4(4).1 he types of activities or conditions considered unusual or unauthorized; and hitors inbound and outbound communications for unusual or unauthorized activities or conditions.	n documentation; information system other relevant documents or o an external information system. Related Controls:

SI-4(5) – Enhancement (Moderate)		
Control		
	f the following types of compromise, or potential compromise, occur:	
(a) Presence of malicious code,		
(b) Unauthorized export of information,(c) Signaling to an external information system,	n r	
(d) Potential intrusions.		
	References: ARS: SI-4(5)	Related Controls:
ASSESSMENT PROCEDURE: SI-4(5).1		
Assessment Objective		
Determine if:	· · · · · · · · · · · · · · ·	
() 5	romise or potential compromise to the security of the information system; and	
	lert when any of the organization-defined list of compromise, or potential compromise indicators occur.	
Assessment Methods And Objects		it, along information overlaps and it air a toolo
	y; procedures addressing information system monitoring tools and techniques; information system secure em configuration settings and associated documentation; other relevant documents or records.(Optional	
Test: Information system monitoring real-time al	5 5 C C C C C C C C C C C C C C C C C C)
SI-4(CMS-1) – Enhancement (Moderate)		
Control		
Install IDS devices at network perimeter points a	nd host-based IDS sensors on critical servers	
Applicability: All	References: ARS: SI-4(CMS-1): IRS-1075: 5.6.2.5#1.1-2. 5.6.2.5#1.4	Related Controls:
ASSESSMENT PROCEDURE: SI-4(CMS-1).1		
Assessment Objective		
Determine if:		
(i) IDS devices are installed at network perimete	r points: and	
(ii) host-based IDS sensors are installed on critic		
Assessment Methods And Objects		
	y; procedures addressing information system monitoring tools and techniques; information system desig	n documentation: information system
	information system configuration settings and associated documentation; other relevant documents or r	
at network perimeter points and host-based IDS	sensors are installed on critical servers.	
Interview: Personnel with system and information	on integrity responsibilities to determine IDS devices are installed at network perimeter points and host-b	ased IDS sensors are installed on critical
servers.		
	n capability to determine IDS devices are installed at network perimeter points and host-based IDS sens	sors are installed on critical servers.
SI-5 – Security Alerts and Advisories (M	loderate)	
Control		
Procedures shall be developed, documented, ar	d implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis	s, and for issuing IS alerts and advisories to
	rts and advisories, personnel shall take appropriate response actions. The types of actions to be taken	in response to security alerts / advisories shall
be documented.		
Guidance	an ba an bar in an ann an an an aite a lanta (an bha air a 🐨 bha ann a tha tha an air air an tha tha an air	
	to be taken in response to security alerts/advisories. The organization also maintains contact with speced information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advide	
	ST SP 800-40 provides guidance on monitoring and distributing security alerts and advisories.	ce from security professionals, and (iii)
Applicability: All	References: ARS: SI-5; NIST 800-53/53A: SI-5; PISP: 4.17.5	Related Controls:
ASSESSMENT PROCEDURE: SI-5.1		,
Assessment Objective		
Determine if:		
(i) the organization receives information system	security alerts/advisories on a regular basis;	
	-	

CMS C	ore Security Requirements for Moderate Impact I	Level Assessments
(ii) the organization issues security alerts/advis	sories to appropriate organizational personnel; and	
(iii) the organization takes appropriate actions		
Assessment Methods And Objects	······································	
	licy; procedures addressing security alerts and advisories; NIST SP 800-40; records	of security alerts and advisories; other relevant documents or
records.		
Interview: Organizational personnel with secu	irity alert and advisory responsibilities; organizational personnel implementing, opera	ating, maintaining, administering, and using the information system.
SI-5(1) – Enhancement (Moderate)		
Control		
Employ automated mechanisms to make secu	rity alerts and advisory information available to all appropriate personnel.	
Applicability: All	References: ARS: SI-5(1)	Related Controls:
ASSESSMENT PROCEDURE: SI-5(1).1		
Assessment Objective		
-	ted mechanisms to make security alert and advisory information available throughou	It the organization as needed.
Assessment Methods And Objects		
Examine: System and information integrity po	licy; procedures addressing security alerts and advisories; information system desig	n documentation; information system configuration settings and
associated documentation; automated mechar records.(Optional)	nisms supporting the distribution of security alert and advisory information; records o	f security alerts and advisories; other relevant documents or
	he distribution of security alert and advisory information.(Optional)	
SI-6 – Security Functionality Verification	on (Moderate)	
Control		
	and implemented effectively to provide the capability for CMS information systems to e actions when security-related anomalies are discovered.	verify the correct operation of security functions on a regular basis
Guidance		
	s to all security functions. For those security functions that are not able to execute at cepts the risk of not performing the verification as required.	utomated self-tests, the organization either implements
Applicability: All	References: ARS: SI-6; NIST 800-53/53A: SI-6; PISP: 4.17.6	Related Controls:
SSESSMENT PROCEDURE: SI-6.1		
Assessment Objective		
Determine if:		
	nditions for conducting security function verification;	
	ity function verification, the frequency of the verifications;	
	m responses to anomalies discovered during security function verification;	
	operation of security functions in accordance with organization-defined conditions and	nd in accordance with organization-defined frequency (if periodic
verification); and	u function anomalias in accordance with arranization defined reasonance	
	y function anomalies in accordance with organization-defined responses.	
Assessment Methods And Objects	lieur presedures addressing accurity function verification; information avetam design	documentation: information austern acquirity plan; information
	licy; procedures addressing security function verification; information system design documentation; other relevant documents or records.(Optional)	documentation, information system security plan, information
Test: Security function verification capability.(
SI-7 – Software and Information Integr		
3		
Control Automated mechanisms for software and infor detect unauthorized changes to software. Goo	mation integrity shall be in place and supporting procedures shall be developed, doo od software engineering practices consistent with CMS IS policy and procedures sha	cumented, and implemented effectively to both protect against and
	isms shall be in place to monitor the integrity of the CMS information system and ap	
Guidance		1
	applications on the information system to look for evidence of information tampering	a, errors, and omissions. The organization employs good software
	ial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks	
	Page 178 of 189	BPSSM Appendix A. Attachmen

Applicability: All	References: ARS: SI-7; FISCAM: TAN-3.1.2, TAN-3.2.1, TAN-3.2.2, TAY-2.1.4, TAY-2.2.2, TCP-	Related Controls:
	2.1.2, TCP-2.1.3, TCP-2.1.4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7; PISP: 4.17.7	
ASSESSMENT PROCEDURE: SI-7.1		
Assessment Objective		
Determine if:		
(i) the information system detects and pre-	otects against unauthorized changes to software and information; and	
(ii) the organization employs effective int	egrity verification tools in accordance with good software engineering practices.	
Assessment Methods And Objects		
	ity policy; procedures addressing software and information integrity; information system design documentation;	information system configuration settings and
	cation tools and applications documentation; other relevant documents or records.(Optional)	
Test: Software integrity protection and ve	erification capability.(Optional)	
SI-7(0) – Enhancement (Moderate)		
Control		
Employ off-the-shelf integrity mechanism	s such as parity checks, check-sums, error detection data validation techniques, cyclical redundancy checks, ar	nd cryptographic hashes to detect and protec
	nissions and unauthorized changes to software and use tools to automatically monitor the integrity of the inform	
Applicability: All	References: ARS: SI-7(0); FISCAM: TAC-3.3; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); PISP: 4.17.7	Related Controls:
ASSESSMENT PROCEDURE: SI-7(0).1		
Assessment Objective		
Determine if the organization meets the	requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ying enhancement to the baseline control.
Assessment Methods And Objects		
Examine: System and information integr	ity policy; procedures addressing software and information integrity; information system design documentation;	information system configuration settings and
	ication tools and applications documentation; other relevant documents or records.	, , , , , , , , , , , , , , , , , , , ,
SI-7(FIS-1) – Enhancement (Moderate)		
Control		
Control	and data is developed that represents the various activities and conditions that will be encountered in processi	ng. Live data are not used in testing of
Control	and data is developed that represents the various activities and conditions that will be encountered in processi a files.	ng. Live data are not used in testing of
Control A comprehensive set of test transactions program changes except to build test dat		ng. Live data are not used in testing of Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All	References: FISCAM: TCC-2.1.6, TCC-2.1.7	
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS	References: FISCAM: TCC-2.1.6, TCC-2.1.7	
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS	References: FISCAM: TCC-2.1.6, TCC-2.1.7	-
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if:	References: FISCAM: TCC-2.1.6, TCC-2.1.7	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe	a files. References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files.	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files.	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures.	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and objects	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures.	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and o SI-7(FIS-2) – Enhancement (Moderate)	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures.	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and of SI-7(FIS-2) – Enhancement (Moderate) Control	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures. quality assurance personnel.	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and o SI-7(FIS-2) – Enhancement (Moderate) Control User-prepared record count and control to	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures.	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and of SI-7(FIS-2) – Enhancement (Moderate) Control User-prepared record count and control to Applicability: All	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures. quality assurance personnel. totals established over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and co SI-7(FIS-2) – Enhancement (Moderate) Control User-prepared record count and control to ASSESSMENT PROCEDURE: SI-7(FIS	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures. quality assurance personnel. totals established over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1	Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and of SI-7(FIS-2) – Enhancement (Moderate) Control User-prepared record count and control f ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures. quality assurance personnel. rotals established over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1 -2).1	Related Controls: be encountered in processing. ssing. Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and of SI-7(FIS-2) – Enhancement (Moderate) Control User-prepared record count and control f ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if the organizational user-prep	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures. quality assurance personnel. totals established over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1	Related Controls: be encountered in processing. ssing. Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and of SI-7(FIS-2) – Enhancement (Moderate) Control User-prepared record count and control f ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if the organizational user-prep Assessment Methods And Objects	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures. quality assurance personnel. totals established over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1 -2).1 wared record count and control totals documents help determine the completeness of data entry and processing.	Related Controls: be encountered in processing. ssing. Related Controls:
Control A comprehensive set of test transactions program changes except to build test dat Applicability: All ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective Determine if: (i) the organization provides a comprehe (ii) the organizational validation does not Assessment Methods And Objects Examine: Pertinent policies and procedu Examine: Test transactions and data. Interview: Programmers, auditors, and of SI-7(FIS-2) – Enhancement (Moderate) Control User-prepared record count and control f ASSESSMENT PROCEDURE: SI-7(FIS Assessment Objective	References: FISCAM: TCC-2.1.6, TCC-2.1.7 -1).1 nsive set of test transactions and data is developed that represents the various activities and conditions that will use live data in testing of program changes except to build test data files. ures. quality assurance personnel. totals established over source documents are used to help determine the completeness of data entry and proce References: FISCAM: TCP-1.1.1 -2).1 wared record count and control totals documents help determine the completeness of data entry and processing.	Related Controls: be encountered in processing. ssing. Related Controls:

Examine: Application documentation.		
Examine: Pertinent policies and procedures.		
Interview: User management and personnel.		
SI-7(FIS-3) – Enhancement (Moderate)		
Control		
For on-line or real-time systems, record count an	d control totals are accumulated progressively for a specific time period	(daily or more frequently) and are used to help determine the completenes
or data entry and processing.		
Applicability: All	References: FISCAM: TCP-1.1.2	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-3).1		
Assessment Objective		
•	e systems, record count and control totals are accumulated progressive	ely for a specific time period (daily or more frequently) and are used to help
determine the completeness or data entry and pr		· · · · · · · · · · · · · · · · · · ·
Assessment Methods And Objects	5	
Examine: Application documentation.		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation generated	by system.	
Interview: Application programmer, if available.		
Interview: User management and personnel.		
SI-7(FIS-4) – Enhancement (Moderate)		
Control		
	over and entered with transaction data, and reconciled to determine the	e completeness of data entry
Applicability: All	References: FISCAM: TCP-2.1.1	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-4).1		Related Controls.
Assessment Objective	d control totals are actablished over and entered with transaction data is	and reconciled to determine the completeness of data entry
	d control totals are established over and entered with transaction data, a	and reconclied to determine the completeness of data entry.
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Pertinent policies and procedures.		
Examine: Reconciliation activities.		
Interview: Data control personnel.		
Interview: User management and personnel.		
SI-7(FIS-5) – Enhancement (Moderate)		
Control		
	completeness of transactions processed, master files updated, and output	5
Applicability: All	References: FISCAM: TCP-2.2.1	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-5).1		
Assessment Objective		
Determine if the organizational reconciliations ar	e performed to determine the completeness of transactions processed, i	master files updated, and outputs generated.
Assessment Methods And Objects		
-		
Examine: Application documentation.		
Examine: Application documentation. Examine: Pertinent policies and procedures.		
Examine: Pertinent policies and procedures.		

SI-8 – Spam Protection (Moderate)		
Control		
	Il be in place at critical information system entry points, workstations, servers, and mobile computing de	wices on the network. Supporting procedures
	ted effectively to both protect against and detect spam.	wices on the network. Supporting procedures
Guidance		
mobile computing devices on the network. The o electronic mail attachments, Internet accesses, o	nanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access rganization uses the spam protection mechanisms to detect and take appropriate action on unsolicited or other common means. Consideration is given to using spam protection software products from multip or for workstations). NIST SP 800-45 provides guidance on electronic mail security.	messages transported by electronic mail,
Applicability: All	References: ARS: SI-8; HIPAA: 164.308(a)(1)(i); NIST 800-53/53A: SI-8; PISP: 4.17.8	Related Controls:
ASSESSMENT PROCEDURE: SI-8.1		
Assessment Objective		
Determine if:		
(i) the information system implements spam protection		
(ii) the organization employs spam protection me	echanisms at critical information system entry points and at workstations, servers, or mobile computing	devices on the network;
(iii) the organization employs spam protection me	echanisms to detect and take appropriate action on unsolicited messages transported by electronic mai	l; and
	echanisms whenever new releases are available in accordance with organizational policy and procedur	
Assessment Methods And Objects		
	u presedures addressing anom protection, information puster design desumentation, anom protection	machaniama, information quatern configuration
settings and associated documentation; other rel	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.	mechanisms, information system configuration
Test: Spam detection and handling capability.		
SI-8(1) – Enhancement (Moderate)		
Control		
Centrally manage spam protection mechanisms.	References: ARS: SI-8(1); HIPAA: 164.308(a)(1)(i)	Related Controls:
	Relefences. Ar.S. SI-0(1), HIPAA. 104.300(a)(1)(1)	Related Collitors.
ASSESSMENT PROCEDURE: SI-8(1).1		
Assessment Objective		
Assessment Objective Determine if the organization centrally manages	spam protection mechanisms.	
Determine if the organization centrally manages	spam protection mechanisms.	
Determine if the organization centrally manages Assessment Methods And Objects		mechanisms: information system configuration
Determine if the organization centrally manages Assessment Methods And Objects	y; procedures addressing spam protection; information system design documentation; spam protection	mechanisms; information system configuration
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity polic settings and associated documentation; other rel	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional)	mechanisms; information system configuration
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity polic	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional)	mechanisms; information system configuration
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policy settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate)	
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policy settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restrictions	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i	
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policy settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restricted beyond the typical access controls emplayed Automated mechanisms shall be in place to restricted beyond the typical access controls emplayed Determine if the organization control access controls emplayed Automated mechanisms shall be in place to restricted beyond the typical access controls emplayed Determine if the organization control access controls emplayed Determine if the organization control access controls employed Determine if the organization control access control access controls employed Determine if the organization control access co	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate)	
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity polici settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restrice restricted beyond the typical access controls em Guidance	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities.	nformation to the information system shall be
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policy settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restricted beyond the typical access controls em Guidance Restrictions on personnel authorized to input information	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i	nformation to the information system shall be
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity polici settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restri- restricted beyond the typical access controls emp Guidance Restrictions on personnel authorized to input info operational/project responsibilities.	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities.	nformation to the information system shall be tem and include limitations based on specific
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policy settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restricted beyond the typical access controls em Guidance Restrictions on personnel authorized to input information	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities. pormation to the information system may extend beyond the typical access controls employed by the syst References: ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2,	nformation to the information system shall be
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity polici settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restri- restricted beyond the typical access controls emp Guidance Restrictions on personnel authorized to input infor- operational/project responsibilities. Applicability: All	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities.	nformation to the information system shall be tem and include limitations based on specific
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policy settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restrice restricted beyond the typical access controls em Guidance Restrictions on personnel authorized to input infor- operational/project responsibilities. Applicability: All ASSESSMENT PROCEDURE: SI-9.1	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities. pormation to the information system may extend beyond the typical access controls employed by the syst References: ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2,	nformation to the information system shall be tem and include limitations based on specific
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policis settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restricted beyond the typical access controls em Guidance Restrictions on personnel authorized to input informational/project responsibilities. Applicability: All ASSESSMENT PROCEDURE: SI-9.1 Assessment Objective	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities. prmation to the information system may extend beyond the typical access controls employed by the syst References: ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.1; NIST 800-53/53A: SI-9; PISP: 4.17.9	nformation to the information system shall be tem and include limitations based on specific
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policis settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restrice restricted beyond the typical access controls em Guidance Restrictions on personnel authorized to input infor- operational/project responsibilities. Applicability: All ASSESSMENT PROCEDURE: SI-9.1 Assessment Objective Determine if the organization restricts the capability	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities. pormation to the information system may extend beyond the typical access controls employed by the syst References: ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2,	nformation to the information system shall be tem and include limitations based on specific
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policis settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restricted beyond the typical access controls em Guidance Restrictions on personnel authorized to input informational/project responsibilities. Applicability: All ASSESSMENT PROCEDURE: SI-9.1 Assessment Objective	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities. prmation to the information system may extend beyond the typical access controls employed by the syst References: ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.1; NIST 800-53/53A: SI-9; PISP: 4.17.9	nformation to the information system shall be tem and include limitations based on specific
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policy settings and associated documentation; other rel SI-9 – Information Input Restrictions (M Control Automated mechanisms shall be in place to restrice restricted beyond the typical access controls em Guidance Restrictions on personnel authorized to input information operational/project responsibilities. Applicability: All ASSESSMENT PROCEDURE: SI-9.1 Assessment Objective Determine if the organization restricts the capability Assessment Methods And Objects	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities. prmation to the information system may extend beyond the typical access controls employed by the syst References: ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.1; NIST 800-53/53A: SI-9; PISP: 4.17.9	nformation to the information system shall be tem and include limitations based on specific Related Controls:
Determine if the organization centrally manages Assessment Methods And Objects Examine: System and information integrity policis settings and associated documentation; other relections of the settings and associated documentation; other relections of the settings and associated documentation; other relections of the settings of the settings and associated documentation; other relections of the settings and associated documentation; other relections on personnel authorized to input informational/project responsibilities. Applicability: All Assessment Objective Determine if the organization restricts the capability and the organization integrity policies of the setting of of	y; procedures addressing spam protection; information system design documentation; spam protection levant documents or records.(Optional) oderate) rict information input to the information system to authorized personnel. Personnel authorized to input i ployed by the system, including limitations based on specific operational / project responsibilities. prmation to the information system may extend beyond the typical access controls employed by the syst References: ARS: SI-9; FISCAM: TAN-2.2.1, TAN-2.2.2, TAY-2.3.1; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.1; NIST 800-53/53A: SI-9; PISP: 4.17.9	nformation to the information system shall be tem and include limitations based on specific Related Controls:

SI-10 – Information Accuracy, Complete	eness, Validity, and Authenticity (Moderate)	
Control		
Automated mechanisms shall verify information	for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.	
Guidance		
Checks for accuracy, completeness, validity, an	d authenticity of information are accomplished as close to the point of origin as possible. Rules for check	ing the valid syntax of information system
	ge, acceptable values) are in place to verify that inputs match specified definitions for format and conten	
	inintentionally interpreted as commands. The extent to which the information system is able to check the	accuracy, completeness, validity, and
authenticity of information is guided by organiza		
Applicability: All	References: ARS: SI-10; FISCAM: TAN-3.1.1, TAY-1.2.1, TAY-1.4.1, TAY-2.1.3, TCP-2.1.2, TCP-2.1.3, TCP-2.1.4; IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-10; PISP: 4.17.10	Related Controls:
ASSESSMENT PROCEDURE: SI-10.1		
Assessment Objective		
Determine if:		
(i) the information system checks information for	r accuracy, completeness, validity, and authenticity;	
	and authenticity of information is accomplished as close to the point of origin as possible;	
	ck the valid syntax of information inputs to verify that inputs match specified definitions for format and co	
	on inputs passed to interpreters to prevent the content from being unintentionally interpreted as commar	ids.
Assessment Methods And Objects		
	cy; procedures addressing information accuracy, completeness, validity, and authenticity; access control	
	nated tools and applications to verify accuracy, completeness, validity, and authenticity of information; inf	ormation system design documentation;
	ssociated documentation; other relevant documents or records.	
	information for accuracy, completeness, validity, and authenticity.(Optional)	
6I-10(CMS-1) – Enhancement (Moderate)		
Control		
Implement automated system checks of informa	tion for accuracy, completeness, validity, and authenticity.	
Applicability: All	References: ARS: SI-10(CMS-1); FISCAM: TAN-3.1.1, TCP-2.1.3, TCP-2.1.4; IRS-1075: 5.6.2.5#1.1-2	Related Controls:
ASSESSMENT PROCEDURE: SI-10(CMS-1).	1	
Assessment Objective		
-	rmation for accuracy, completeness, validity, and authenticity.	
Assessment Methods And Objects		
	cy; procedures addressing information accuracy, completeness, validity, and authenticity; access control	policy and procedures: separation of duties
	nated tools and applications to verify accuracy, completeness, validity, and authenticity of information; inf	
	ssociated documentation; other relevant documents or records to determine that automated system chec	ks of information for accuracy, completeness
validity, and authenticity are performed.		
	on integrity responsibilities to determine that automated system checks of information for accuracy, comp	pleteness, validity, and authenticity are
performed.		
	mated system checks of information for accuracy, completeness, validity, and authenticity are performed	1.
6I-10(FIS-1) – Enhancement (Moderate)		
Control		
The source document is well-designed to aid the numbers, transaction types and field codes are	e preparer and facilitate data entry and includes document pre-numbering and preprinting of transaction entered into the system to facilitate completeness and sequence checking. Access to blank source docu	type and data field codes. The document uments is restricted to authorized personnel.
pplicability: All	References: FISCAM: TAN-1.1.1, TAN-1.1.2, TAN-1.1.3, TAY-1.1.1, TAY-1.1.2, TCP-1.2.1	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-1).1		
Assessment Objective		
-		
Determine if the organizational source documen		Investigation of transportion time and date for
	t is well-designed to aid the preparer and facilitate data entry and includes document pre-numbering and as and field codes are entered into the system to facilitate completeness and sequence checking. Access	

authorized personnel. Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Blank document storage area. Examine: Procedures for recording and tracking of numbers if pre-numbered documents are used. Examine: Source documents and data entry activities. Interview: User management and personnel.	
 Examine: Pertinent policies and procedures. Examine: Blank document storage area. Examine: Procedures for recording and tracking of numbers if pre-numbered documents are used. Examine: Source documents and data entry activities. Interview: User management and personnel. 	
Examine: Blank document storage area. Examine: Procedures for recording and tracking of numbers if pre-numbered documents are used. Examine: Source documents and data entry activities. Interview: User management and personnel.	
Examine: Procedures for recording and tracking of numbers if pre-numbered documents are used. Examine: Source documents and data entry activities. Interview: User management and personnel.	
Examine: Source documents and data entry activities. Interview: User management and personnel.	
Interview: User management and personnel.	
SI-10(FIS-2) – Enhancement (Moderate)	
Control	
For batch application systems, a batch control sheet is prepared for a group of source documents, and includes: date, control n identification of the user submitting the batch.	number, number of documents, a control total for a key field, and
Applicability: All References: FISCAM: TAN-1.1.4	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-2).1	
Assessment Objective	
Determine if the organizational batch application systems prepared a batch control sheet for a group of source documents, and	d includes: date, control number, number of documents, a control total
for a key field, and identification of the user submitting the batch.	
Assessment Methods And Objects	
Examine: Pertinent policies and procedures.	
Examine: Batch control sheets if batch application.	
Examine: Prepared source documents and batches if batch application.	
Interview: Users responsible for preparing batch control sheets and submitting the batch.	
SI-10(FIS-3) – Enhancement (Moderate)	
Control	
Key source documents require authorizing signatures. Data control unit personnel: verify that source documents are properly p source documents.	prepared and authorized; and monitor data entry and processing of
Applicability: All References: FISCAM: TAN-1.2.1, TAN-1.2.2	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-3).1	
Assessment Objective	
Determine if the organizational key source documents require authorizing signatures. Data control unit personnel: verify that so	purce documents are properly prepared and authorized; and monitor
data entry and processing of source documents.	
Assessment Methods And Objects	
Examine: Key source documents and data entry activities.	
Examine: Pertinent policies and procedures.	
Interview: Management and data control unit personnel.	
SI-10(FIS-4) – Enhancement (Moderate)	
Control	
Supervisory or control unit personnel review data and enter an authorizing code before data is released for processing.	
Applicability: All References: FISCAM: TAN-1.2.3	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-4).1	
Assessment Objective	
Determine if the organizational supervisory or control unit personnel review data and enter an authorizing code before data is re-	released for processing.
Assessment Methods And Objects	· · · · · · · · · · · · · · · · · · ·
Examine: Pertinent policies and procedures.	
Examine: Review process.	
Interview: Management and data control unit personnel.	

SI-10(FIS-5) – Enhancement (Moderate)		
Control		
	oplication so that the action can be analyzed for appropriateness and correctness.	
Applicability: All	References: FISCAM: TAY-2.3.2	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-5).1		
Assessment Objective		
o i	n override is automatically logged by the application so that the action can be ana	lyzed for appropriateness and correctness.
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Override audit logs.		
Interview: Application programmer, if available,	, and user management personnel.	
SI-10(FIS-6) – Enhancement (Moderate)		
Control		
, ,	rs are automatically assigned a unique sequence number, which is used by the co	
Applicability: All	References: FISCAM: TCP-1.2.2	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-6).1		
Assessment Objective		
Determine if the organizational information syste that all transactions are processed.	em transactions without preassigned serial numbers are automatically assigned a	unique sequence number, which is used by the computer to monitor
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation generated		
Interview: Application programmer, if available.		
Interview: User management and personnel.		
6I-10(FIS-7) – Enhancement (Moderate)		
Control		
Transactions are sequence checked and compu produced, and items are investigated and resolv	uter matched with data in master or suspense files to identify missing or duplicate ved in a timely manor.	transactions. Reports of missing or duplicate transactions are
Applicability: All	References: FISCAM: TCP-1.2.3, TCP-1.2.4, TCP-1.3.1, TCP-1.3.2	Related Controls:
ASSESSMENT PROCEDURE: SI-10(FIS-7).1		
Assessment Objective		
Determine if the organizational information syste	em transactions are sequence checked and computer matched with data in maste produced, and items are investigated and resolved in a timely manor.	er or suspense files to identify missing or duplicate transactions.
Assessment Methods And Objects		
Examine: Activity to investigate items reported	as missing or duplicate.	
Examine: Application documentation.	······································	
Examine: Pertinent policies and procedures.		
Examine: Reports of missing and duplicate tran	nsactions.	
Interview: Application programmer, if available.		
Interview: User management and personnel.		
SI-10(FIS-8) – Enhancement (Moderate)		
SI-10(FIS-8) – Enhancement (Moderate) Control Individual transactions or source documents are	e compared with a detailed listing of items processed by the computer, particularly	to control important low-volume, high-value transactions.

Assessment Objective				
Determine if the organizational ir	formation system's individual transaction	s or source documents are compared with a c	detailed listing of items processed	by the computer, particularly to control
important low-volume, high-value				
Assessment Methods And Obje	cts			
Examine: Comparison activity.				
0	showing checking was performed.			
Examine: Pertinent policies and	procedures.			
Interview: User management ar	d personnel.			
SI-11 – Error Handling (Mod	erate)			
Control				
	t could be exploited by adversaries. Syst	litious manner. User error messages generat tem error messages shall be revealed only to		
Guidance				
system provide timely and usefu	information without revealing potentially rs) are not listed in error logs or associate	he organization. Error messages are revealed harmful information that could be used by adv ed administrative messages. The extent to wh	versaries. Sensitive information (e	.g., account numbers, social security
Applicability: All	References: ARS: SI-11	1; FISCAM: TAY-3.2.1; NIST 800-53/53A: SI-	11; PISP: 4.17.11	Related Controls: SI-2
ASSESSMENT PROCEDURE: S	I-11.1			
 (ii) the information system reveal (iii) the information system does Assessment Methods And Obje Examine: System and information associated documentation; other Test: Information system error h SI-11(0) – Enhancement (Model Control Employ automated mechanisms 	s only essential information to authorized not include sensitive information in error l ects on integrity policy; procedures addressing relevant documents or records. andling capability.(Optional) ate) that generate error messages providing ti count numbers, User IDs, social security r References: ARS: SI-11	logs or associated administrative messages.	on system design documentation; revealing information that could b	information system configuration settings and e exploited by adversaries. Ensure
Assessment Objective	ato the requirements on apositied in the h	populing control and the apopulity CMC requires	monto on proporihad in this amplify	ing ophonooment to the baseline ecotrol
-		paseline control and the specific CMS requirer	nents as prescribed in this amplity	ying enhancement to the baseline control.
Assessment Methods And Obje		information and an annual baseling information		
examine: System and information associated documentation; other		i information system error handling; information	on system design documentation;	information system configuration settings and
SI-11(FIS-1) – Enhancement (M				
Control				
Rejected data are automatically	s processed and the error identified, and illing transactions processed.	ile and purged as corrected. Each erroneous (3) the identity of the user who originated the		
Applicability: All	References: FISCAM: T	ГАҮ-3.1.1, ТАҮ-3.1.2, ТАҮ-3.1.4		Related Controls:
Rev. 9		Page 185 of 189		BPSSM Appendix A, Attachment 2

ASSESSMENT PROCEDURE: SI-10(FIS-8).1

ASSESSMENT PROCEDURE: SI-11(FIS-1).1	
Assessment Objective	
Determine if the organizational information system's rejected data is automatically written on an automated error suspense file and purged as corrected	
(1) codes indicating the type of data error, (2) date and time the transaction was processed and the error identified, and (3) the identity of the user who	originated the transaction. Record counts and
control totals are established over the suspense file and used in reconciling transactions processed.	
Assessment Methods And Objects	
Examine: Application documentation and interview application programmers, if available.	
Examine: Reports produced from the suspense file.	
Interview: User management and personnel.	
Test: Verify process with test transactions containing errors.	
SI-11(FIS-2) – Enhancement (Moderate)	
Control	
A control group is responsible for: reviewing suspense file control total reports, determining completeness of processing, and controlling and monitoring	rejected transactions
Applicability: All References: FISCAM: TAY-3.1.3	Related Controls:
ASSESSMENT PROCEDURE: SI-11(FIS-2).1	
Assessment Objective	
Determine if the organizational information system's control group is responsible for: reviewing suspense file control total reports, determining complete	ness of processing, and controlling and
monitoring rejected transactions	
Assessment Methods And Objects	
Examine: Pertinent policies and procedures.	
Examine: Reports produced from the suspense file.	
Interview: User management and control group.	
Test: Verify review process with test transactions containing errors.	
SI-11(FIS-3) – Enhancement (Moderate)	
Control	
The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age	of uncorrected transactions.
Applicability: All References: FISCAM: TAY-3.1.5	Related Controls:
ASSESSMENT PROCEDURE: SI-11(FIS-3).1	
Assessment Objective	
Determine if:	
(i) the organizational information system [The suspense file] is produced, on a regular basis for management review; and	
(ii) the organization determines the level and type of transaction errors and the age of uncorrected transactions.	
Assessment Methods And Objects	
Examine: Analysis reports produced from the suspense file.	
Examine: Application documentation.	
Examine: Pertinent policies and procedures.	
Interview: User management and control group.	
SI-11(FIS-4) – Enhancement (Moderate)	
Control	
Errors are corrected by the user originating the transaction, and all corrections are reviewed and approved by supervisors before the corrections are ree	entered.
Applicability: All References: FISCAM: TAY-3.2.2, TAY-3.2.3	Related Controls:
ASSESSMENT PROCEDURE: SI-11(FIS-4).1	
Assessment Objective	
Determine if the organizational information system errors are corrected by the user originating the transaction, and all corrections are reviewed and app	roved by supervisors before the corrections are
reentered.	source by supervisors before the corrections are
romotod.	

Rev. 9

Assessment Methods And Objects		
Examine: Error correction activities.		
Examine: Error reports. Examine: Pertinent policies and procedures.		
Interview: User management and personnel.		
Test: Verify test transactions containing errors.		
SI-11(FIS-5) – Enhancement (Moderate)		
Control		
A control group is responsible for: reviewing cor	trol total reports, determining completeness of processing, and controlling and monitoring rejected trans	actions
Applicability: All	References: FISCAM: TCP-2.1.5	Related Controls:
ASSESSMENT PROCEDURE: SI-11(FIS-5).1		
Assessment Objective		
	responsible for: reviewing control total reports, determining completeness of processing, and controlling	and monitoring rejected transactions
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Pertinent policies and procedures.		
Examine: Review and completeness of process	sing activities.	
Interview: Data control personnel.		
Interview: User management and personnel. SI-12 – Information Output Handling and	d Potention (Moderate)	
	a Retention (Moderate)	
Control		
information sensitivity level.	ed and retained in accordance with applicable laws, Executive Orders, directives, policies, regulations, s	tandards, operational requirements, and the
Guidance		
A good place to obtain procedures for handling		
Applicability: All	References: ARS: SI-12; FISCAM: TAY-4.1.6; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2; NIST 800- 53/53A: SI-12; PISP: 4.17.12	Related Controls:
ASSESSMENT PROCEDURE: SI-12.1		
Assessment Objective		
Determine if:		
 (i) the organization handles and retains output fi requirements; and 	rom the information system in accordance with applicable laws, Executive Orders, directives, policies, re	gulations, standards, and operational
(ii) the organization handles output from the info	ormation system in accordance with labeled or marked instructions on information system output (includi tion, distribution, transport, or storage of information system output.	ng paper and digital media) that includes, but
Assessment Methods And Objects		
Examine: System and information integrity polic other relevant documents or records.	cy; procedures addressing information system output handling and retention; media protection policy and	d procedures; information retention records,
Interview: Organizational personnel with inform	ation output handling and retention responsibilities.(Optional)	
SI-12(CMS-1) – Enhancement (Moderate)		
Control		
Retain output, including, but not limited to audit applicable National Archives and Records Admi	records, system reports, business and financial reports, and business records, from the information syst nistration (NARA) requirements.	em in accordance with CMS Policy and all
Applicability: All	References: ARS: SI-12(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2	Related Controls:
ASSESSMENT PROCEDURE: SI-12(CMS-1).	1	· · · · · · · · · · · · · · · · · · ·
Assessment Objective		
Determine if the organization retains output, incl accordance with CMS Policy and all applicable	luding, but not limited to audit records, system reports, business and financial reports, and business reco NARA requirements.	ords, from the information system in
Rev. 9	Page 187 of 189	BPSSM Appendix A, Attachment

Examine: At a minimum, documentation for record retention audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements are met.

SI-12(FIS-1) – Enhancement (Moderate)

Control

Responsibility is assigned for seeing that all outputs are produced and distributed according to system requirements and design by a data processing control group, or some alternative. A data processing control group: (1) has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; (2) reviews output products for general acceptability: and (3) reconciles control information to determine completeness of processing.

Applicability: All	References: FISCAM: TAY-4.1.1, TAY-4.1.2	Related Controls:
ASSESSMENT PROCEDU	RE: SI-12(FIS-1).1	
Assessment Objective		
Determine if the organizat	ion assigns responsibility for seeing that all outputs are produced and distributed according to syste	em requirements and design by a data processing control group, or some
	sing control group: (1) has a schedule by application that shows when outputs should be completed	
	t products for general acceptability; and (3) reconciles control information to determine completene	ess of processing.
Assessment Methods And		
Examine: Output product		
Examine: Pertinent policie		
	stem and user management.	
SI-12(FIS-2) – Enhanceme	nt (Moderate)	
Control		
Printed reports contain a t	itle page with report name, time and date of production, the processing period covered; and have a	an "end-of-report" message.
Applicability: All	References: FISCAM: TAY-4.1.3	Related Controls:
ASSESSMENT PROCEDU	RE: SI-12(FIS-2).1	
Assessment Objective		
Determine if the organizat	ional information system printed reports contain a title page with report name, time and date of pro	duction, the processing period covered; and have an "end-of-report"
message.		
Assessment Methods And	d Objects	
Examine: Application doc	umentation.	
Examine: Printed reports.		
Interview: User personne	l and application programmer, if available.	
SI-12(FIS-3) – Enhanceme	nt (Moderate)	
Control		
Each output produced, wh	nether printed or transmitted to a user's terminal device, is logged, manually if not automatically, inc	cluding the recipient(s) who receive the output.
Applicability: All	References: FISCAM: TAY-4.1.4, TAY-4.1.5	Related Controls:
ASSESSMENT PROCEDU	RE: SI-12(FIS-3).1	
Assessment Objective		
-	ional information system's output produced, whether printed or transmitted to a user's terminal dev	rice, is logged, manually if not automatically, including the recipient(s) who
receive the output.		
Assessment Methods And	d Objects	
Examine: Application doc	umentation.	
Examine: Output logs.		
Interview: Information sys	stem and user personnel.	
SI-12(FIS-4) – Enhanceme	nt (Moderate)	
Control		

Control

In the user department, outputs transmitted are summarized daily and printed for each terminal device, and reviewed by supervisors. A control log of output product errors is maintained, including the corrective actions take.

Applicability: All	References: FISCAM: TAY-4.1.7, TAY-4.1.8	Related Controls:
ASSESSMENT PROCEDURE:	SI-12(FIS-4).1	
Assessment Objective		
	I information system's user department, outputs transmitted are summarized daily and printed for ained, including the corrective actions take.	or each terminal device, and reviewed by supervisors. A control log of
Assessment Methods And Ob	ojects	
Examine: Pertinent policies ar	nd procedures.	
Examine: Supporting docume	ntation (e.g., printed daily summaries with supervisory initials or signatures).	
Examine: This activity.		
Interview: User supervisory pe	ersonal.	
SI-12(FIS-5) – Enhancement (I	Moderate)	
· · · · · · · · · · · · · · · · · · ·	Moderate)	
Control	Moderate) r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transactic	on reports, (3) master record change reports, (4) exception reports, an
Control Users review output reports for (5) control totals balance report	· · · · · ·	n reports, (3) master record change reports, (4) exception reports, an
	r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transactic	on reports, (3) master record change reports, (4) exception reports, an Related Controls:
Control Users review output reports for (5) control totals balance report	r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction rts. Output from reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1	
Control Users review output reports for (5) control totals balance repor Applicability: All	r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction rts. Output from reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1	
Control Users review output reports for (5) control totals balance repor Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organizational	r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction rts. Output from reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1	Related Controls:
Control Users review output reports for (5) control totals balance repor Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organizational	r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction rts. Output from reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1 SI-12(FIS-5).1 I users review output reports for data accuracy, validity, and completeness. The reports includes and (5) control totals balance reports. Output from reruns is subjected to the same quality review	Related Controls:
Control Users review output reports for (5) control totals balance repor Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organizational reports, (4) exception reports, i	r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction rts. Output from reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1 SI-12(FIS-5).1 I users review output reports for data accuracy, validity, and completeness. The reports include: and (5) control totals balance reports. Output from reruns is subjected to the same quality revier ojects	Related Controls:
Control Users review output reports for (5) control totals balance report Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organizational reports, (4) exception reports, a Assessment Methods And Ob	r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction rts. Output from reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1 SI-12(FIS-5).1 I users review output reports for data accuracy, validity, and completeness. The reports include: and (5) control totals balance reports. Output from reruns is subjected to the same quality revier ojects	Related Controls: : (1) error reports, (2) transaction reports, (3) master record change
Control Users review output reports for (5) control totals balance repor Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organizational reports, (4) exception reports, i Assessment Methods And Ob Examine: Activity to review out	r data accuracy, validity, and completeness. The reports include: (1) error reports, (2) transaction rts. Output from reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1 SI-12(FIS-5).1 I users review output reports for data accuracy, validity, and completeness. The reports include: and (5) control totals balance reports. Output from reruns is subjected to the same quality revier ojects utput reports.	Related Controls: : (1) error reports, (2) transaction reports, (3) master record change

Business Partners Systems Security Manual

Appendix A, Attachment 3

CMS Core Security Requirements (CSR)

for

Low Impact Level Assessments



CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

Rev. 9

(This page intentionally left blank)

Access Control (AC) – Technical

AC-1 – Access Control Policy and Procedures (Low)

Control

Logical access controls and procedures shall be established and implemented effectively to ensure that only designated individuals, under specified conditions (e.g. time of day, port of entry, type of authentication) can access the CMS information system, activate specific commands, execute specific programs and procedures, or create views or modify specific objects (i.e., programs, information, system parameter). Procedures shall be developed to guide the implementation and management of logical access controls. The logical access controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and shall be periodically reviewed, and, if necessary, updated.

Guidance

The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075; 5.6.3.2#1; NIST 800-53/53A; AC-1; PISP; 4.1.1	
Applicability: All	References: ARS: AC-1; FISCAM: TAC-3.2.C.1, TAC-4.3.4, TSD-1.1.1, TSD-2.1, TSS-1.1.1; HIPAA:	Related Controls:

ASSESSMENT PROCEDURE: AC-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents access control policy and procedures;

(ii) the organization disseminates access control policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review access control policy and procedures; and

(iv) the organization updates access control policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities.(Optional)

ASSESSMENT PROCEDURE: AC-1.2

Assessment Objective

Determine if:

(i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

- (ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and
- (iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.

Interview: Organizational personnel with access control responsibilities.(Optional)

AC-1(FIS-1) – Enhancement (Low)

Control

Standard forms are used to document approval for archiving, deleting, or sharing data files. Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.

Applicability: All	References: FISCAM: TAC-2.3.1, TAC-2.3.2	Related Controls:
ASSESSMENT PROCEDURE: AC-1(FIS-1).1		

Assessment Objective

Determine if:

(i) the organization uses standard forms to document approval for archiving, deleting, or sharing data files; and

(ii) the organizational agreements, with other entities, document prior to sharing data or programs how the data files are protected.

Assessment Methods And Objects

Examine: Documents authorizing file sharing and file sharing agreements.

Examine: Pertinent policies and procedures.

Examine: Standard approval forms.

Interview: Data owners.

AC-2 – Account Management (Low)

Control

Comprehensive account management mechanisms shall be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. Access to the CMS information system shall be granted based on: (a) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (b) intended system usage. Proper identification and approval shall be required for requests to establish information system accounts.

Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to authorize and monitor the use of guest / anonymous accounts; and to remove, disable, or otherwise secure unnecessary accounts. Account managers shall be notified when CMS information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers shall also be notified when users' information system usage or need-to-know changes.

Guidance

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system usage or need-to-know/need-to-share changes.

Applicability: All	References: ARS: AC-2; FISCAM: TAC-3.2.C.4, TAC-3.2.C.5, TSP-4.1.6, TSS-1.1.3; HIPAA:	Related Controls:
	164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1; NIST 800-	
	53/53A: AC-2; PISP: 4.1.2	

ASSESSMENT PROCEDURE: AC-2.1

Assessment Objective

Determine if:

(i) the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts;

(ii) the organization defines the frequency of information system account reviews;

(iii) the organization reviews information system accounts at the organization-defined frequency, at least annually; and

(iv) the organization initiates required actions on information system accounts based on the review.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing account management; information system security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.

Interview: Organizational personnel with account management responsibilities.(Optional)

interview. Organizational personna		
AC-2(0) – Enhancement (Low)		
Control		
Review information system account	s every 365 days and require annual certification.	
Applicability: All	References: ARS: AC-2(0); FISCAM: TAC-3.2.C.4, TSS-1.1.4; HIPAA: 164.308(a)(3)(ii)(B),	Related Controls:
	164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#2.1; NIST 800-53/53A: AC-2; PISP: 4.1.2	
ASSESSMENT PROCEDURE: AC-	2(0).1	
Assessment Objective		
Determine if the organization meets	the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this an	nplifying enhancement to the baseline control.
Assessment Methods And Object	S S S S S S S S S S S S S S S S S S S	
	count management procedures; information system security plan (for organization-defined account review freque employees; list of recently disabled information system accounts; system-generated records with user IDs and la	

Interview: Organizational personnel with account management responsibilities.(Optional)

AC-2(CMS-1) – Enhancement (Low)

Control

Remove or disable default user accounts. Rename active default accounts.

 Applicability: All
 References: ARS: AC-2(CMS-1); FISCAM: TAC-3.2.A.3, TAC-3.2.C.4, TSS-1.2.3; IRS-1075:
 Related Controls:

ASSESSMENT DROCEDURE AS SOME A	5.6.3.2#2.1	
ASSESSMENT PROCEDURE: AC-2(CMS-1).		
Assessment Objective		
	ion system accounts, including establishing, activating, modifying, reviewing, disabling, and removing ac	ccounts.
Assessment Methods And Objects		
accounts if they must be used.	s; other relevant documents or records to determine if the organization removes or disables default user	
Interview: Organizational personnel with acces renamed.	s control responsibilities to determine that all default user accounts are either removed or disabled. If de	efault accounts are active, that they are
AC-2(CMS-2) – Enhancement (Low)		
Control		
Require the use of unique and separate adminis	strator accounts for administrator and non-administrator activities.	
Applicability: All	References: ARS: AC-2(CMS-2); FISCAM: TAN-2.1.4; IRS-1075: 5.6.3.2#2.1	Related Controls: IA-4(CMS-1)
ASSESSMENT PROCEDURE: AC-2(CMS-2).	1	
Assessment Objective		
	paration of duties through assigned access authorizations.	
Assessment Methods And Objects		
	gement procedures; information system security plan (for organization-defined account review frequency	(); list of active user and system accounts; list
	list of recently disabled information system accounts; system-generated records with user IDs and last I	ogin date; other relevant documents or records
	strator accounts to be used for day-to-day activities.	
	nt management responsibilities to determine if administrator accounts are being used for day to day acti	vities.
AC-2(CMS-3) – Enhancement (Low)		
Control		
Implement centralized control of user access ad	ministrator functions.	
Applicability: All	References: ARS: AC-2(CMS-3); IRS-1075: 5.6.3.2#2.1	Related Controls:
ASSESSMENT PROCEDURE: AC-2(CMS-3).	1	
Assessment Objective		
Determine if the organization manages informat	ion system accounts, including establishing, activating, modifying, reviewing, disabling, and removing ac	ccounts.
Assessment Methods And Objects		
Examine: Access control policy; account manage	gement procedures; information system security plan (for organization-defined account review frequency	/); list of active user and system accounts; list
of recently separated or terminated employees; to determine if all user access administrator fund	list of recently disabled information system accounts; system-generated records with user IDs and last I ctions are centralized.	ogin date; other relevant documents or records
Interview: Organizational personnel with accou	nt management responsibilities to determine if all user access administrator functions are carried out by	a centralized administrator function.
AC-2(CMS-4) – Enhancement (Low)		
Control		
Regulate the access provided to contractors and	d define security requirements for contractors.	
Applicability: All	References: ARS: AC-2(CMS-4); IRS-1075: 5.6.3.2#2.1	Related Controls:
ACCESSIONENT DROOFDURE. AC ACOMO A	1	
ASSESSMENT PROCEDURE: AC-2(CMS-4).		
ASSESSMENT PROCEDURE: AC-2(CMS-4). Assessment Objective		
Assessment Objective	ctor security requirements and maintains contractor access privileges.	
Assessment Objective		
Assessment Objective Determine if the organization documents contra Assessment Methods And Objects	ctor security requirements and maintains contractor access privileges.	 /); list of active user and system accounts: list
Assessment Objective Determine if the organization documents contra Assessment Methods And Objects Examine: Access control policy; account manager of recently separated or terminated employees;		

Interview: Organizational personnel with account management responsibilities to determine if written authorizations exist for a sample of contractor employees.

AC-2(CMS-5) – Enhancei	nent (Low)	
Control		
Revoke employee acces	s rights upon termination. Physical access and system access must be revoked immediately	
Applicability: All	References: ARS: AC-2(CMS-5); FISCAM: TSP-4.1.6; IRS-1075: 5	5.6.3.2#2.1 Related Controls:
ASSESSMENT PROCED	JRE: AC-2(CMS-5).1	
Assessment Objective		
Determine if the organization	ation terminates information system access upon termination of individual employment.	
Assessment Methods Ar	nd Objects	
	ol policy; account management procedures; information system design documentation; inform	nation system configuration settings and associated documentation; other relevan
	determine when employee access rights are revoked on termination.	
5	al personnel with personnel security responsibilities to determine when access is revoked on	employee termination.
AC-2(FIS-1) – Enhancem	ent (Low)	
Control		
All system access autho	rizations are: (1) documented on standard forms and maintained on file, (2) approved by sen	nior managers, and (3) securely transferred to security managers.
Guidance		
	owner should identify the specific user or class of users that are authorized to obtain direct a	ccess to each resource for which he or she is responsible. This process can be
simplified by developing	standard profiles, which describe access needs for groups of users with similar duties.	
Applicability: All	References: FISCAM: TAC-2.1.1, TAC-2.2	Related Controls:
ASSESSMENT PROCED	JRE: AC-2(FIS-1).1	
Assessment Objective		
Determine if:		
(i) the organization grant	s system access authorizations on standard forms and maintains the completed forms on file	e; and
(ii) the organizational se	nior managers approve system access authorizations and the approvals are securely transfe	erred to security managers.
Assessment Methods Ar	Id Objects	
Examine: Pertinent police		
	ser (both application user and information system personnel) access authorization document	itation.
	volved in access authorizations and senior managers who approve authorizations.	
AC-2(FIS-2) – Enhancem	ent (Low)	
Control		
	lically review system access authorization listings and determine whether they remain approp	priate. ISSO/SSOs review system access authorizations and discuss any
	ons with Business Owners.	
Applicability: All	References: FISCAM: TAC-2.1.2, TAC-2.1.4	Related Controls:
ASSESSMENT PROCED	JRE: AC-2(FIS-2).1	
Assessment Objective		
Determine if the organization	ation security managers periodically reviews system access authorization listings and discus	ses questionable authorizations with management.
Assessment Methods Ar	1d Objects	
Examine: Access autho	rization listings to determine whether inappropriate access are removed in a timely manner.	
Examine: Pertinent polic	vies and procedures.	
	ners and review supporting documentation. Determine whether inappropriate access is reme	loved in a timely manner.
· · · · · · · · · · · · · · · · · · ·	agers and review documentation provided to them.	
AC-2(3) – Enhancement	(Low)	
Control		
	n system to disable inactive accounts automatically after 365 days.	

ASSESSMENT PROCEDURE: AC-2(3).1

Assessment Objective

Determine if:

(i) the organization defines a time period after which the information system disables inactive accounts; and

(ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.

Assessment Methods And Objects

Examine: Procedures addressing account management; information system security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records. **Test:** Automated mechanisms implementing account management functions.(Optional)

AC-3 – Access Enforcement (Low)

Control

Access enforcement mechanisms shall be developed, documented and implemented effectively to control access between named users (or processes) and named objects (e.g., files and programs) in a CMS information system. Additional application level access enforcement mechanism shall be implemented, when necessary, to provide increased information security for CMS information. When encryption of stored information is employed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (see section 4.16.13).

Guidance

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

Applicability: All	References: ARS: AC-3; FISCAM: TAC-3.2.C.1, TAC-3.2.C.5, TAC-3.2.C.6, TAC-3.2.D.1, TCC-3.2.3,	Related Controls: MA-CMS-1, MA-CMS-2,
	TSS-2.1.1, TSS-2.1.2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3;	SC-13
	NIST 800-53/53A: AC-3; PISP: 4.1.3	

ASSESSMENT PROCEDURE: AC-3.1

Assessment Objective

Determine if:

(i) the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy; and

(ii) user privileges on the information system are consistent with the documented user authorizations.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records.

Test: Automated mechanisms implementing access enforcement policy.(Optional)

AC-3(1) – Enhancement (Low)

Control

Ensure the information system restricts access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.

Guidance

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Applicability: All	References: ARS: AC-3(1); FISCAM: TAC-3.2.C.1, TAC-3.2.C.2, TAC-3.2.C.5, TAC-3.2.D.1, TCC-	Related Controls:
	3.2.3, TSD-3.1.4, TSS-1.1.2, TSS-2.1.2	

ASSESSMENT PROCEDURE: AC-3(1).1

Assessment Objective

Determine if:

(i) the organization explicitly defines privileged functions and security-relevant information for the information system;

(ii) the organization explicitly authorizes personnel access to privileged functions and security-relevant information in accordance with organizational policy; and

(iii) the information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel (e.g., security administrators).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; list of privileged functions and security relevant information; information system configuration settings and associated documentation: list of assigned authorizations (user privileges); information system audit records; other relevant documents or records. (Optional) Test: Automated mechanisms implementing access enforcement policy.(Optional)

AC-3(CMS-1) – Enhancement (Low)

Control

If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Applicability: All	References: ARS: AC-3(CMS-1)	Related Controls: SC-13
ASSESSMENT PROCEDURE: AC-3(CMS-1).1		

Assessment Objective

Determine if for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if encryption is used as an access control mechanism, examine system and communications protection policy: procedures addressing use of cryptography: FIPS 140-2 (as amended): NIST SP 800-56 and 800-57; information system design documentation: information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

Interview: Organizational personnel with access control responsibilities to determine if the organization's encryption standard meets CMS-approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13, Use of Cryptography, PISP 4.16.13).

AC-3(CMS-2) – Enhancement (Low)

Control

If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix A for e-Authentication Standards.

Applicability: All	References: ARS: AC-3(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: AC-3(CMS-2).		

Assessment Objective

Determine if the information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records if e-authentication is used as an access control mechanism, examine Identification and authentication policy. NIST SP 800-63: procedures addressing user identification and authentication: information system design documentation: information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the organization's encryption standard meets ARS Appendix A for e-Authentication Standards.

Interview: Organizational personnel with access control responsibilities if e-authentication is used as an access control mechanism, interview system administrators responsible for the hosts providing authentication services to determine if the organization meets the standards described in ARS Appendix A.

AC-3(CMS-3) – Enhancement (Low)

Control

Configure operating system controls to disable public "write" access to files, objects, and directories that may directly impact system functionality and/or performance.

Applicability: All	References: ARS: AC-3(CMS-3); FISCAM: TAC-3.2.D.1, TCC-3.2.3; IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-3(CMS-3).1		

Assessment Objective

Determine if the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements.

Assessment Methods And Objects

Examine: Access enforcement policy and procedures; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges): information system audit records: other relevant documents or records to determine if operating system controls are configured to disable public "read" and "write" access to all system files, objects, and directories. Operating system controls must be configured to disable public "read" access to files, objects, and directories that contain sensitive information.

	control responsibilities to determine if operating system controls are configured to disable public "read" a be configured to disable public "read" access to files, objects, and directories that contain sensitive inforr	
AC-5 – Separation of Duties (Low)		
support functions shall be divided among differer not also administer audit functions). Personnel d	prced to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. Mission fu t roles, and support functions shall be performed by different individuals (e.g., personnel responsible for eveloping and testing system code shall not have access to production libraries. Access control softwar f two or more individuals is required to commit fraudulent activity. Job descriptions shall reflect accurate	administering access control functions shall e shall be in place to limit individual authority
Guidance The organization establishes appropriate division control software on the information system that p of duties include: (i) mission functions and distinct	is of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities revents users from having all of the necessary authority or information access to perform fraudulent activ t information system support functions are divided among different individuals/roles; (ii) different individu ogramming, quality assurance/testing, configuration management, and network security); and (iii) securit	vity without collusion. Examples of separation als perform information system support
Applicability: All	References: ARS: AC-5; FISCAM: TAY-1.3.2, TSD-1.1.1, TSD-1.1.2, TSD-1.1.3, TSD-1.1.5, TSD-1.2.1, TSD-1.3.3, TSD-2.2.2, TSS-1.1.2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3; NIST 800-53/53A: AC-5; PISP: 4.1.5	Related Controls:
ASSESSMENT PROCEDURE: AC-5.1		
 (ii) the information system enforces separation of Assessment Methods And Objects Examine: Access control policy; procedures add information system audit records; other relevant of 	ressing separation of duties; information system configuration settings and associated documentation; lis documents or records.(Optional) sibilities for defining appropriate divisions of responsibility and separation of duties.(Optional)	
AC-5(CMS-1) – Enhancement (Low)		
Control Ensure that audit functions are not performed by	security personnel responsible for administering access control.	
Applicability: All	References: ARS: AC-5(CMS-1); FISCAM: TAC-2.1.5	Related Controls:
ASSESSMENT PROCEDURE: AC-5(CMS-1).1		
Assessment Objective Determine if the organization establishes approp Assessment Methods And Objects	riate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the res	ponsibilities and duties of individuals.
records; other relevant documents or records to or enforces separation of duties through assigned a Interview: Organizational personnel with response	dures; information system configuration settings and associated documentation; list of separation of dutie determine if audit functions are NOT performed by security personnel responsible for administering acce access authorizations. sibilities for defining appropriate divisions of responsibility and separation of duties to determine if audit f ons complement and reinforce separation of duties.	ss control. Also, ensure that the organization
AC-5(CMS-2) – Enhancement (Low)		
	ccess based upon the users' roles and responsibilities.	
Applicability: All	References: ARS: AC-5(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: AC-5(CMS-2).1		
Assessment Objective Determine if the organization establishes approp	riate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the res	ponsibilities and duties of individuals.
Rev. 9	Page 7 of 127	BPSSM Appendix A, Attachment 3

Assessment Methods And Objects

Examine: Separation of duties policy and procedures; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records to determine if the organization maintains a limited group of administrators with access based upon the users' roles and responsibilities. Interview: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties to determine if the number of personnel with root access is limited to only those personnel with a business poor for root access is limited.

to only those personnel with a business need for	root access.	
AC-5(CMS-3) – Enhancement (Low)		
Control		
Ensure that critical mission functions and information	ation system support functions are divided among separate individuals.	
Applicability: All	References: ARS: AC-5(CMS-3); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-5(CMS-3).1		
Assessment Objective		
Determine if the organization establishes approp	riate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibility and separates duties as needed to eliminate conflicts of interest in the response of the second	sponsibilities and duties of individuals.
Assessment Methods And Objects		
	dures; information system configuration settings and associated documentation; list of separation of dution	
	determine if the organization ensures that critical mission functions and information system support func	
	sibilities for defining appropriate divisions of responsibility and separation of duties to determine if the or	ganization ensures that critical mission
functions and information system support function	ins are divided among separate individuals.	
AC-5(CMS-4) – Enhancement (Low)		
Control		
	(i.e., user acceptance, quality assurance, information security) and production functions are divided amo	
Applicability: All	References: ARS: AC-5(CMS-4); FISCAM: TSD-1.1.2; IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-5(CMS-4).1		
Assessment Objective		
Determine if the organization establishes approp	priate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the res	sponsibilities and duties of individuals.
Assessment Methods And Objects		
	dures; information system configuration settings and associated documentation; list of separation of dution	
	determine if information system testing functions (i.e., user acceptance, quality assurance, information s	ecurity) and production functions are divided
among separate individuals or groups.		
	isibilities for defining appropriate divisions of responsibility and separation of duties to determine that info	irmation system testing functions (i.e., user
	rity) and production functions are divided among separate individuals or groups.	
AC-5(FIS-1) – Enhancement (Low)		
Control		
	adequate resources and training to ensure that segregation of duty principles are understood and estab	ished, enforced, and institutionalized within
the organization.	Peterences FICOANA TOD 4 0.0	Deleted Controles
Applicability: All ASSESSMENT PROCEDURE: AC-5(FIS-1).1	References: FISCAM: TSD-1.3.2	Related Controls:
Assessment Objective		e i i i i i i i i i i i i i i
Determine if the organization provides adequate organization.	resources and training to ensure that segregation of duty principles are understood and established, en	orced, and institutionalized within the
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
	or management has provided adequate resources and training to establish, enforce, and institutionalize	the principles of segregation of duties
AC-6 – Least Privilege (Low)		and principles of segregation of duties.
Control	t restrictive set of privileges peopled for the performance of sutherized tasks	
□ active user or process shall be assigned the mos	t restrictive set of privileges needed for the performance of authorized tasks.	

Outlands		
Guidance		
	east privilege for specific duties and information systems (including specific ports, protocols, and services) in a rganizational operations, organizational assets, and individuals.	accordance with risk assessments as
Applicability: All	References: ARS: AC-6; FISCAM: TSD-2.1; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); HSPD 7:	Related Controls:
Applicability. All	D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2; NIST 800-53/53A: AC-6; PISP: 4.1.6	Related Controls.
ASSESSMENT PROCEDURE: AC-6.1		
Assessment Objective		
Determine if:		
(i) the organization assigns the most restri	ctive set of rights/privileges or accesses needed by users for the performance of specified tasks; and	
	ost restrictive set of rights/privileges or accesses needed by users.	
Assessment Methods And Objects		
documentation; information system audit r	es addressing least privilege; list of assigned access authorizations (user privileges); information system confi ecords; other relevant documents or records.(Optional)	guration settings and associated
	responsibilities for defining least privileges necessary to accomplish specified tasks.(Optional)	
AC-6(CMS-1) – Enhancement (Low)		
Control		
Disable all file system access not explicitly	required for system, application, and administrator functionality.	
Applicability: All	References: ARS: AC-6(CMS-1); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-6(CM	S-1).1	
Assessment Objective		
Determine if the information system enfore	ces separation of duties through assigned access authorizations.	
Assessment Methods And Objects		
	es addressing least privilege; list of assigned access authorizations (user privileges); information system confi	
functionality is disabled.	ecords; other relevant documents or records to determine if all file system access not explicitly required for system	
determine if file system access not explicit	responsibilities for defining least privileges necessary to accomplish specified tasks to determine hosts that sto Ily required for system, application, and administrator functionality are disabled.	ore, transmit or process sensitive data to
AC-6(CMS-2) – Enhancement (Low)		
Control		
contractor's ability to adhere to and suppo		selection process must assess the
Applicability: All	References: ARS: AC-6(CMS-2); HSPD 7: D(10); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: AC-6(CM	S-2).1	
Assessment Objective		
Determine if the information system enfor	ces separation of duties through assigned access authorizations.	
Assessment Methods And Objects		
	es addressing least privilege; list of assigned access authorizations (user privileges); information system confi	
	ecords; other relevant documents or records to determine if contractors are required to be provided with minim	
	ty requirements. The documented contractor selection process must assess the contractor's ability to adhere to	
	responsibilities for defining least privileges necessary to accomplish specified tasks to determine the default ac d for system, application, and administrator functionality is disabled.	ccess levels given to contractors. Ensure that
AC-6(CMS-3) – Enhancement (Low)		
Control	utilities to only outhorized detabase administrators	
Applicability: All	utilities to only authorized database administrators. References: ARS: AC-6(CMS-3); FISCAM: TAC-3.2.D.1, TAC-3.2.D.2, TAC-3.2.D.3, TAC-3.2.D.4	Related Controls:

ASSESSMENT PROCEDURE: AC-6(CMS-3).1 **Assessment Objective** Determine if the information system enforces separation of duties through assigned access authorizations. Assessment Methods And Objects Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the information system restricts the use of database management utilities to only authorized database administrators. Policies and procedures must also prevent users from accessing database data files at the logical data view, field, or field-value levels. Implement column-level access controls. Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks to determine if the information system restricts the use of database management utilities to only authorized database administrators. Also, determine whether or not users are prevented from accessing database data files at the logical data view, field, or field-value levels. Column-level access controls must also be implemented. AC-7 – Unsuccessful Log-on Attempts (Low) Control Automated mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enforce a limit of CMS-defined consecutive invalid access attempts by a user during a specified time period. Systems shall be locked after a specified number of multiple unsuccessful log-on attempts. Guidance Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. Applicability: All References: ARS: AC-7; IRS-1075: 5.6.3.2#4.1; NIST 800-53/53A: AC-7; PISP: 4.1.7 **Related Controls: ASSESSMENT PROCEDURE: AC-7.1** Assessment Objective Determine if: (i) the organization defines the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur: (ii) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period; (iii) the organization defines the time period for lock out mode or delay period; (iv) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts: and (v) the information system enforces the organization-selected lock out mode or delayed login prompt. **Assessment Methods And Objects** Examine: Access control policy; procedures addressing unsuccessful logon attempts; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts.(Optional) AC-7(0) – Enhancement (Low) Control Configure the information system to disable access for at least five (5) minutes after three (3) failed log-on attempts by a user during a five (5) minute time period. Applicability: All References: ARS: AC-7(0): IRS-1075: 5.6.3.2#4.1: NIST 800-53/53A: AC-7: PISP: 4.1.7 Related Controls: AC-9 ASSESSMENT PROCEDURE: AC-7(0).1 **Assessment Objective** Determine if the organization configures system lockout to assist in preventing password guessing. **Assessment Methods And Objects** Examine: Password lockout policy includes failed log-on attempts, lockout timeframes period for failed attempts and system/network administrator account reset capabilities. Interview: A sampling of users for knowledge of log-on and account lockout procedure policy is known. AC-8 – System Use Notification (Low) Control An approved warning / notification message shall be displayed upon successful log-on and before gaining system access. The warning message shall notify users that the CMS information system is owned by the U.S. Government and shall describe conditions for access, acceptable use, and access limitations. The system use notification message shall provide appropriate privacy and security

notices (based on associated privacy and securit	ty policies) and shall remain on the screen until the user takes explicit actions to log-on to the CMS inforr	nation system
Guidance		
Privacy and security policies are consistent with in the form of warning banners displayed when ir displayed before granting access; (ii) any referer	applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use individuals log in to the information system. For publicly accessible systems: (i) the system use information nees to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems to a system includes a description of the authorized uses of the system.	n is available and when appropriate, is
Applicability: All	References: ARS: AC-8; FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2; NIST 800-53/53A: AC-8; PISP: 4.1.8	Related Controls: SI-4
ASSESSMENT PROCEDURE: AC-8.1		
Assessment Objective		
 that the user is accessing a U.S. Government in that system usage may be monitored, recorded that unauthorized use of the system is prohibite that use of the system indicates consent to mor (ii) the system use notification message provides (iii) the organization approves the information system (iv) the system use notification message remains Assessment Methods And Objects Examine: Access control policy; procedures address other relevant documents or records.	l, and subject to audit; ed and subject to criminal and civil penalties;	
AC-8(CMS-1) – Enhancement (Low)		
 (a) They are accessing a U.S. Government inform (b) CMS maintains ownership and responsibility (c) Users must adhere to CMS Information Seculid) (d) Their usage may be monitored, recorded, and (e) Unauthorized use is prohibited and subject to 	for its computer systems; rity Policies, Standards, and Procedures; d audited;	
Guidance	, , ,	
All CMS information system computers and netw	ork devices under their control, independently, prominently and completely display the notice and conse mited to, web, ftp, telnet, or other services accessed.	nt banner immediately upon users'
Applicability: All	References: ARS: AC-8(CMS-1); FISCAM: TAC-3.2.E.2.1; IRS-1075: 5.6.3.2#4.2	Related Controls:
ASSESSMENT PROCEDURE: AC-8(CMS-1).1		
Assessment Objective		
 that the user is accessing a U.S. Government in that system usage may be monitored, recorded that unauthorized use of the system is prohibite that use of the system indicates consent to more 	l, and subject to audit; ed and subject to criminal and civil penalties;	
Assessment Methods And Objects		the second second second state of the second state of the

(c) Users must adhere to CMS Information Security Policies, Standards, and Procedures;

Interview: Organizational personnel to determin (a) They are accessing a U.S. Government infor (b) CMS maintains ownership and responsibility (c) Users must adhere to CMS Information Secu (d) Their usage may be monitored, recorded, an (e) Unauthorized use is prohibited and subject to (f) The use of the information system establishes AC-8(CMS-2) – Enhancement (Low) Control	o criminal and civil penalties; and s their consent to any and all monitoring and recording of their activities. e if hosts are configured to present a warning banner at system access points. The warning banner m mation system; for its computer systems; rity Policies, Standards, and Procedures; d audited; o criminal and civil penalties; and s their consent to any and all monitoring and recording of their activities.	ust contain the following elements:
Develop and implement the warning banner in c Applicability: All	References: ARS: AC-8(CMS-2); IRS-1075: 5.6.3.2#4.2	Related Controls:
ASSESSMENT PROCEDURE: AC-8(CMS-2).1		Related Controls:
Assessment Objective	e provides appropriate privacy and security notices (based on associated privacy and security policies	
Assessment Methods And Objects	e provides appropriate privacy and security notices (based on associated privacy and security policies	or summanes).
	Iressing system use notification; information system notification messages; information system configu	ation settings and associated documentation:
	e if warning banners were developed and implemented in conjunction with legal counsel.	
	e if warning banners were developed and implemented in conjunction with legal counsel.	
AC-8(CMS-3) – Enhancement (Low)		
Control		
Post clear privacy policies on web sites, major e	ntry points to a web site and any web page where substantial personal information from the public is co	llected.
Applicability: All	References: ARS: AC-8(CMS-3); IRS-1075: 5.6.3.2#4.2	Related Controls:
ASSESSMENT PROCEDURE: AC-8(CMS-3).1		
Assessment Objective		
Determine if the system use notification messag	e provides appropriate privacy and security notices (based on associated privacy and security policies	or summaries).
Assessment Methods And Objects		
other relevant documents or records to determin public is collected.	Iressing system use notification; information system notification messages; information system configu e if clear privacy policies are posted on web sites, major entry points to a web site and any web page v	here substantial personal information from the
	e if clear privacy policies are posted where substantial personal information from the public is collected	
AC-13 – Supervision and Review—Acce	ss Control (Low)	
Control		
Personnel shall be supervised and reviewed with and any unusual activities shall be investigated i and responsibilities shall be reviewed more frequ	n respect to the usage of CMS information system access controls. Automated mechanisms shall be in n a timely manner. Changes to access authorizations shall be reviewed periodically. The activities of Jently.	place to facilitate the review of audit records, users with significant information system roles
Guidance		
system-related activities and periodically reviews responsibilities. The extent of the audit record re reviewed frequently for every workstation, but ra provides guidance on computer security log mar		h significant information system roles and stems, it is not intended that security logs be
Applicability: All	References: ARS: AC-13; FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSD-3.2.1, TSD-3.2.3, TSS-	Related Controls:

ASSESSMENT PROCEDURE:	: AC-13.1	
Assessment Objective		
	supervises and reviews the activities of users with respect to the enforcement and usage of information system acces	es controls
Assessment Methods And Ol		
	cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o	of supervisory potices of disciplinary actions to
	ception reports; other relevant documents or records.	
	sonnel with supervisory and access control responsibilities.(Optional)	
AC-13(CMS-1) – Enhancemer	ht (Low)	
Control		
	irectories for unexpected and/or unauthorized changes at least once per day. Automate the review of file creation, cha	anges and deletions: and monitor permission
	fication for technical staff review and assessment.	
Applicability: All	References: ARS: AC-13(CMS-1); FISCAM: TAC-2.1.5; HIPAA: 164.312(c)(2), 164.312(e)(2)(i)	Related Controls:
ASSESSMENT PROCEDURE:	: AC-13(CMS-1).1	
Assessment Objective		
-	employs automated mechanisms within the information system to support and facilitate the review of user activities.	
Assessment Methods And Ol		
	cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o	of supervisory notices of disciplinary actions to
	reption reports; other relevant documents or records to determine if files and directories are reviewed for unexpected a	
	anges and deletions, and permission changes must be monitored automatically. Alert notifications must be generated	
	sonnel with supervisory and access control responsibilities to determine if the integrity of files and directories for unex	
	ation, changes and deletions, and permission changes are being reviewed automatically. Determine if alert notification	ns for technical staff review and assessment are
being generated.		
AC-13(CMS-2) – Enhancemer	it (Low)	
Control		
00 0	or and user account activities, system shutdowns, reboots, errors and access authorizations.	Related Controls:
Applicability: All	References: ARS: AC-13(CMS-2); FISCAM: TAC-2.1.5, TAN-2.1.8, TSS-2.1.3	Related Controls
		Related Controls.
ASSESSMENT PROCEDURE:		
ASSESSMENT PROCEDURE: Assessment Objective	: AC-13(CMS-2).1	
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of	EXC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities.	
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol	: AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects	
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ob Examine: Access control police	: AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o	of supervisory notices of disciplinary actions to
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ob Examine: Access control polic users; information system exc	: AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects	of supervisory notices of disciplinary actions to
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled.	: AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o ception reports; other relevant documents or records to determine if logging of administrator and user account activities	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled.	: AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o ception reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o seption reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led.	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enable AC-13(CMS-3) – Enhancemen	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o seption reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led.	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enable AC-13(CMS-3) – Enhancemen Control	: AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o ception reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led. nt (Low)	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enable AC-13(CMS-3) – Enhancemen Control	 AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records or ception reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led. nt (Low) 	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enable AC-13(CMS-3) – Enhancemer Control Inspect administrator groups,	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o ception reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led. nt (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that un References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and nauthorized accounts have not been created.
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enabled AC-13(CMS-3) – Enhancement Control Inspect administrator groups, I	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o ception reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led. nt (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that un References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and nauthorized accounts have not been created.
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enable AC-13(CMS-3) – Enhancement Control Inspect administrator groups, I Applicability: All ASSESSMENT PROCEDURE: Assessment Objective	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o ception reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led. nt (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that un References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and nauthorized accounts have not been created.
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enable AC-13(CMS-3) – Enhancement Control Inspect administrator groups, I Applicability: All ASSESSMENT PROCEDURE: Assessment Objective	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o seption reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led. nt (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that un References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3 : AC-13(CMS-3).1 employs automated mechanisms within the information system to support and facilitate the review of user activities.	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and nauthorized accounts have not been created.
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enabled AC-13(CMS-3) – Enhancemer Control Inspect administrator groups, Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o seption reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account at led. nt (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that us References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3 : AC-13(CMS-3).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; information system desi	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and nauthorized accounts have not been created. Related Controls:
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enabled AC-13(CMS-3) – Enhancemer Control Inspect administrator groups, Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic configuration settings and ass	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o ception reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account activities not (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that un References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3 : AC-13(CMS-3).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; information system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system counts and review of access control enforcement and usage; information system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system cesses control enforcement and usage; information system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system cesses	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and nauthorized accounts have not been created. Related Controls:
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enabled AC-13(CMS-3) – Enhancemer Control Inspect administrator groups, Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic configuration settings and ass demand, but at least once ever	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o seption reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led. nt (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that un References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3 : AC-13(CMS-3).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; information system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and or ery thirty (30) days to ensure that unauthorized accounts have not been created.	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and <u>nauthorized accounts have not been created.</u> Related Controls: gn documentation; information system other system related accounts are inspected on
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enabled AC-13(CMS-3) – Enhancemer Control Inspect administrator groups, Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic configuration settings and ass demand, but at least once ever	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o ception reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account activities not (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that un References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3 : AC-13(CMS-3).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; information system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system counts and review of access control enforcement and usage; information system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system cesses control enforcement and usage; information system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system cesses control enforcement and usage; information system desi	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and <u>nauthorized accounts have not been created.</u> Related Controls: gn documentation; information system other system related accounts are inspected on
ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic users; information system exc authorizations is enabled. Interview: Organizational pers access authorizations is enabled. AC-13(CMS-3) – Enhancemer Control Inspect administrator groups, Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if the organization of Assessment Methods And Ol Examine: Access control polic configuration settings and ass demand, but at least once ever	AC-13(CMS-2).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; organizational records o seption reports; other relevant documents or records to determine if logging of administrator and user account activities sonnel with supervisory and access control responsibilities to determine if logging of administrator and user account a led. nt (Low) root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that un References: ARS: AC-13(CMS-3); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-2.1.5, TSS-2.1.3 : AC-13(CMS-3).1 employs automated mechanisms within the information system to support and facilitate the review of user activities. bjects cy; procedures addressing supervision and review of access control enforcement and usage; information system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and other system desi sociated documentation; other relevant documents or records to determine if administrator groups, root accounts and or ery thirty (30) days to ensure that unauthorized accounts have not been created.	of supervisory notices of disciplinary actions to s, system shutdowns, reboots, errors and access activities, system shutdowns, reboots, errors and <u>nauthorized accounts have not been created.</u> Related Controls: gn documentation; information system other system related accounts are inspected on

demand but at least once every thirty (30) days	to ensure that unauthorized accounts have not been created.	
AC-13(FIS-1) – Enhancement (Low)		
Control		
	te duties have compensating controls, such as supervisory review of transactions performed.	
Applicability: All	References: FISCAM: TSD-1.1.4	Related Controls:
ASSESSMENT PROCEDURE: AC-13(FIS-1).1		Related Controls.
Assessment Objective	annel review transportions portermed	
Determine if the organizational supervisory pers	onnei review transactions performed.	
Assessment Methods And Objects Examine: Activities and test transaction reviews		
Examine: Pertinent policies and procedures.	h.	
Interview: Management.		
AC-14 – Permitted Actions without Iden	tification or Authentication (Low)	
	ublic access to CMS information systems without identification and authorization shall be limited to public figured to permit public access only to the extent necessary to accomplish mission objectives, without find the the strent necessary to accomplish mission objectives.	
Guidance		
The organization allows limited user activity with	out identification and authentication for public websites or other publicly available information systems (e	e.g., individuals accessing a federal
information system at http://www.firstgov.gov).		
Applicability: All	References: ARS: AC-14; NIST 800-53/53A: AC-14; PISP: 4.1.14	Related Controls: IA-2
ASSESSMENT PROCEDURE: AC-14.1		
Assessment Methods And Objects Examine: Access control policy; procedures add information system security plan; other relevant	iments specific user actions that can be performed on the information system without identification or aut dressing permitted actions without identification and authentication; information system configuration sett documents or records. access control policy for permitted actions without identification and authentication.(Optional)	
Control		
	"in storage," "in process," and "in transit" with special dissemination handling or distribution instructions,	in a manner consistent with this policy
Guidance		in a manner consistent with this policy.
Automated labeling refers to labels employed or	n internal data structures (e.g., records, files) within the information system. Information labeling is accom g, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.	plished in accordance with: (i) access control
Applicability: All	References: ARS: AC-16; NIST 800-53/53A: AC-16; PISP: 4.1.16	Related Controls: AC-15
ASSESSMENT PROCEDURE: AC-16.1		
Assessment Objective		
Determine if the information system appropriate	y labels information in storage, in process, and in transmission.	
Assessment Methods And Objects		
Examine: Access control policy; procedures add	dressing automated (internal) labeling of information within the information system; information system de	esign documentation; information system
	ation; other relevant documents or records.(Optional)	
	omated (internal) labeling within the information system.(Optional)	
AC-16(CMS-1) – Enhancement (Low)		
Control		
If automated information labeling is utilized, ensities is labeled as such and instructs / requires special	ure that information in storage, in process, and in transmission is labeled appropriately and in accordance al handling).	e with CMS policy (e.g., sensitive information

Applicability: All	References: ARS: AC-16(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: AC-16(C	CMS-1).1	
Assessment Objective		
Determine if the information system app	propriately labels information in storage, in process, and in transmission.	
Assessment Methods And Objects		
configuration settings and associated do and in transmission is labeled appropriat Interview: Organization personnel to de	dures addressing automated (internal) labeling of information within the information system; information system o ocumentation; other relevant documents or records to determine, if automated information labeling is utilized, en itely and in accordance with CMS policy (e.g., sensitive information is labeled as such and instructs / requires sp etermine, if automated information labeling is utilized, that information in storage, in process, and in transmission tion is labeled as such and instructs / requires special handling).	sure that information in storage, in process, pecial handling).
AC-17 – Remote Access (Low)		
Control		
	shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in wr ho can access the information system from remote locations shall be limited and justification / approval for such	
Dial-up lines, other than those with FIPS the CIO or his/her designated representa up capabilities.	S 140 (as amended) validated cryptography, shall not be used to gain access to a CMS information system that tative, provides specific written authorization. Periodic monitoring shall be implemented to ensure that installed e	processes CMS sensitive information unless equipment does not include unanticipated dial-
Guidance		
Internet). Examples of remote access me specifically designed for public access. T unauthorized connections or subversion federal Personal Identity Verification (PIV	anizational information system by a user (or an information system) communicating through an external, non-org nethods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upor n of authorized connections (e.g., using virtual private network technology). NIST SP 800-63 provides guidance o V) credential is used as an identification token where cryptographic token-based access control is employed, the 800-73 and 800-78. NIST SP 800-77 provides guidance on IPSec-based virtual private networks.	s other than public web servers or systems n source of request) or protects against on remote electronic authentication. If the
Applicability: All	References: ARS: AC-17; FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5, 5.7.1#1; NIST 800-	Related Controls: IA-2, SC-9
	53/53A: AC-17; PISP: 4.1.17	
ASSESSMENT PROCEDURE: AC-17.1		
Assessment Objective		
Determine if the organization documents	s, monitors, and controls all methods of remote access to the information system.	
Assessment Methods And Objects		
Examine: Access control policy; procedu	lures addressing remote access to the information system; information system configuration settings and associ	ated documentation; information system audit
records; other relevant documents or rec		
	th remote access authorization, monitoring, and control responsibilities.(Optional)	
AC-17(4) – Enhancement (Low)		
Control		
	ctions only for compelling operational needs and document the rationale for such access in the security plan for	
		· · · · · · · · · · · · · · · · · · ·
	References: ARS: AC-17(4); FISCAM: TAC-2.1.3, TSS-1.2.4; IRS-1075: 5.6.3.2#5	Related Controls:
ASSESSMENT PROCEDURE: AC-17(4		
ASSESSMENT PROCEDURE: AC-17(4 Assessment Objective		
ASSESSMENT PROCEDURE: AC-17(4 Assessment Objective Determine if: (i) the organization defines the situations (ii) the organization permits remote acce Assessment Methods And Objects	4).1 s and compelling operational needs when remote access to privileged functions on the information system is all ess for privileged functions only for compelling operational needs and documents the rationale for such access in	Related Controls: owed; and n the security plan for the information system.
 (i) the organization defines the situations (ii) the organization permits remote acce Assessment Methods And Objects Examine: Access control policy; procedu security plan; information system audit re 	4).1 s and compelling operational needs when remote access to privileged functions on the information system is allo	Related Controls: owed; and n the security plan for the information system.

AC-17(CMS-1) – Enhancement	t (Low)	
Control		
	rotocols through a VPN link(s) if connected to the information system and using remote administration	
Applicability: All	References: ARS: AC-17(CMS-1); IRS-1075: 5.6.3.2#5	Related Controls: SC-13
ASSESSMENT PROCEDURE:	AC-17(CMS-1).1	
Assessment Objective		
Determine if the organization de	locuments, monitors, and controls all methods of remote access to the information system.	
Assessment Methods And Ob		
	y; procedures addressing remote access to the information system; list of information system accou	
	stem audit records; other relevant documents or records to determine if secure management protoc e enabled. Confirm that an approved encryption standard (see SC-13, Use of Cryptography, PISP 4	
	token-based) is required to access system.	
	sonnel with remote access authorization, monitoring, and control responsibilities to determine if secu	are management protocols through a VPN link(s) if connected to the
	remote administration are enabled. Confirm that an approved encryption standard (see SC-13, Use	
authentication or additional aut	thentication protection (e.g., token-based) is required to access system.	
AC-17(CMS-2) – Enhancement	t (Low)	
Control		
Implement password protection	n for remote access connections.	
Applicability: All	References: ARS: AC-17(CMS-2); IRS-1075: 5.6.3.2#5	Related Controls:
ASSESSMENT PROCEDURE:	AC-17(CMS-2).1	
Assessment Objective		
Determine if the organization d	locuments, monitors, and controls all methods of remote access to the information system.	
Assessment Methods And Ob	vjects	
	by; procedures addressing remote access to the information system; list of information system account	unts; information system configuration settings and associated
documentation; information sys	stem audit records; other relevant documents or records to determine if password protection for rem	note access connections is implemented.
	connel with remote access authorization, monitoring, and control responsibilities to determine if pass	sword protection is required for remote access connections.
AC-17(CMS-3) – Enhancement	t (Low)	
Control		
	h re-authentication to verify connections from authorized locations when the Medicare Data Commu	inications Network (MDCN) cannot be used.
Require callback capability with Applicability: All	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	inications Network (MDCN) cannot be used. Related Controls:
Require callback capability with	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	
Require callback capability with Applicability: All	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	
Require callback capability with Applicability: All ASSESSMENT PROCEDURE:	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if:	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5	
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines mar	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1	
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines mar	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points.	
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines mar (ii) the information system control Assessment Methods And Ob Examine: Access control policy	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. ojects xy; procedures addressing remote access to the information system; list of information system account	Related Controls:
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: A Assessment Objective Determine if: (i) the organization defines mar (ii) the information system control Assessment Methods And Ob Examine: Access control policy documentation; information system	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. bjects xy; procedures addressing remote access to the information system; list of information system accouster audit records; other relevant documents or records to determine if the information system required	Related Controls:
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contr Assessment Methods And Ob Examine: Access control policy documentation; information sys from authorized locations when	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. bjects xy; procedures addressing remote access to the information system; list of information system account for managed access; other relevant documents or records to determine if the information system require the vendor to log	Related Controls: unts; information system configuration settings and associated uires callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contr Assessment Methods And Ob Examine: Access control policy documentation; information sys from authorized locations when enter the network through the s	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. bjects xy; procedures addressing remote access to the information system; list of information system accounts and trecords; other relevant documents or records to determine if the information system require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs are applicated and logged. User IDs are applicated and logged.	Related Controls: unts; information system configuration settings and associated irres callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and ssigned to vendors will be recertified annually.
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contri Assessment Methods And Ob Examine: Access control policy documentation; information syst from authorized locations when enter the network through the s Interview: Organizational person	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. pjects xy; procedures addressing remote access to the information system; list of information system accounts and trecords; other relevant documents or records to determine if the information system require the vendor to lostandard authentication process. Access to such systems will be authorized and logged. User IDs account with remote access authorization, monitoring, and control responsibilities to determine if the information if the information is the information in the information process.	Related Controls: unts; information system configuration settings and associated irres callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and ssigned to vendors will be recertified annually. nformation system requires callback capability with re-authentication
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contri Assessment Methods And Ob Examine: Access control policy documentation; information syst from authorized locations when enter the network through the s Interview: Organizational perso to verify connections from authorized locations from authorized locations authorized locations authorized locations from authorized locati	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. ojects ey; procedures addressing remote access to the information system; list of information system require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs are sonnel with remote access authorization, monitoring, and control responsibilities to determine if the information if the information if the information is the remote access authorization.	Related Controls: unts; information system configuration settings and associated iires callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and ssigned to vendors will be recertified annually. nformation system requires callback capability with re-authenticatior quire the vendor to log-on, the vendor should be assigned a User ID
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contri Assessment Methods And Ob Examine: Access control policy documentation; information system enter the network through the se Interview: Organizational person to verify connections from author and password and enter the network the se	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. ojects ey; procedures addressing remote access to the information system; list of information system require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs as connel with remote access authorization, monitoring, and control responsibilities to determine if the information if the information if the information is that require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs as connel with remote access authorization, monitoring, and control responsibilities to determine if the information is that repetition when MDCN cannot be used. For application systems and turnkey systems and turnkey systems that repetition and the standard authentication process. Access to such systems and turnkey systems that repetition is the information is a sonnel with remote access authorization, monitoring, and control responsibilities to determine if the information is the informatio	Related Controls: unts; information system configuration settings and associated iires callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and ssigned to vendors will be recertified annually. nformation system requires callback capability with re-authenticatior quire the vendor to log-on, the vendor should be assigned a User ID
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contr Assessment Methods And Ob Examine: Access control policy documentation; information sys from authorized locations when enter the network through the s Interview: Organizational person to verify connections from author and password and enter the network AC-17(CMS-4) – Enhancement	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. ojects ey; procedures addressing remote access to the information system; list of information system require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs as connel with remote access authorization, monitoring, and control responsibilities to determine if the information if the information if the information is a general authentication process. Access to such systems and turnkey systems and turnkey systems that require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs as connel with remote access authorization, monitoring, and control responsibilities to determine if the information is that remote access authorization process. Access to such systems and turnkey systems that remote access that remote access authorization, monitoring, and control responsibilities to determine if the information is the information systems and turnkey systems that remote access authorization, monitoring, and control responsibilities to determine if the information is the informatis and is the informatis and is the informatis and i	Related Controls: unts; information system configuration settings and associated iires callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and ssigned to vendors will be recertified annually. nformation system requires callback capability with re-authenticatior quire the vendor to log-on, the vendor should be assigned a User ID
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contr Assessment Methods And Ob Examine: Access control policy documentation; information sys from authorized locations when enter the network through the s Interview: Organizational perso to verify connections from author and password and enter the network AC-17(CMS-4) – Enhancement	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. ojects xy; procedures addressing remote access to the information system; list of information system require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs account with remote access authorization, monitoring, and control responsibilities to determine if the information if the information if the information systems that require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs account with remote access authorization, monitoring, and control responsibilities to determine if the information if the information is that reprise the vendor to log the remote access authorization process. Access to such systems and turnkey systems that repaired locations when MDCN cannot be used. For application systems and turnkey systems that repaired locations when MDCN cannot be used. For application systems and turnkey systems that repaired locations when MDCN cannot be used. For application systems should be authorized at to reprive the top of the standard authentication process. Access to such systems should be authorized at the authorized and log authorized at the authorized at the standard authentication process. Access to such systems should be authorized at top of the standard authentication process. Access to such systems should be authorized at top of the standard authentication process. Access to such systems should be authorized at top of the standard authentication proceses. Access to such systems should be authorized at the	Related Controls: unts; information system configuration settings and associated uires callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and ssigned to vendors will be recertified annually. nformation system requires callback capability with re-authenticatior quire the vendor to log-on, the vendor should be assigned a User ID and logged. User IDs assigned to vendors will be recertified annually
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contr Assessment Methods And Ob Examine: Access control policy documentation; information sys from authorized locations when enter the network through the s Interview: Organizational person to verify connections from author and password and enter the network AC-17(CMS-4) – Enhancement If e-authentication is implement	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. Djects wy; procedures addressing remote access to the information system; list of information system require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs at sonnel with remote access authorization, monitoring, and control responsibilities to determine if the information if the information if the information authentication process. Access to such systems and turnkey systems that require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs at sonnel with remote access authorization, monitoring, and control responsibilities to determine if the information if the information when MDCN cannot be used. For application systems and turnkey systems that repaired locations when MDCN cannot be used. For application systems should be authorized at the authorized at the authorized at the standard authentication process. Access to such systems should be authorized at the authorized at the authorized at the authorized at the standard authentication process. Access to such systems should be authorized at the authorized at the standard authentication process. Access to such systems should be authorized at the authorized at the standard authentication process. Access to such systems should be authorized at the authorized at the standard authentication process. Access to such systems should be authorized at the authorized at the standard authentication process. Access to such systems should be authorized at the authorized at the standard	Related Controls: unts; information system configuration settings and associated irres callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and ssigned to vendors will be recertified annually. nformation system requires callback capability with re-authentication quire the vendor to log-on, the vendor should be assigned a User ID and logged. User IDs assigned to vendors will be recertified annually wuthentication standards.
Require callback capability with Applicability: All ASSESSMENT PROCEDURE: Assessment Objective Determine if: (i) the organization defines mar (ii) the information system contr Assessment Methods And Ob Examine: Access control policy documentation; information sys from authorized locations when enter the network through the s Interview: Organizational person to verify connections from author and password and enter the network AC-17(CMS-4) – Enhancement	References: ARS: AC-17(CMS-3); FISCAM: TAN-2.1.7; IRS-1075: 5.6.3.2#5 AC-17(CMS-3).1 naged access control points for remote access to the information system; and trols all remote accesses through a limited number of managed access control points. ojects xy; procedures addressing remote access to the information system; list of information system require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs account with remote access authorization, monitoring, and control responsibilities to determine if the information if the information if the information systems that require the vendor to log standard authentication process. Access to such systems will be authorized and logged. User IDs account with remote access authorization, monitoring, and control responsibilities to determine if the information if the information is that reprise the vendor to log the remote access authorization process. Access to such systems and turnkey systems that repaired locations when MDCN cannot be used. For application systems and turnkey systems that repaired locations when MDCN cannot be used. For application systems and turnkey systems that repaired locations when MDCN cannot be used. For application systems should be authorized at to reprive the top of the standard authentication process. Access to such systems should be authorized at the authorized and log authorized at the authorized at the standard authentication process. Access to such systems should be authorized at top of the standard authentication process. Access to such systems should be authorized at top of the standard authentication process. Access to such systems should be authorized at top of the standard authentication proceses. Access to such systems should be authorized at the	Related Controls: unts; information system configuration settings and associated uires callback capability with re-authentication to verify connections g-on, the vendor should be assigned a User ID and password and ssigned to vendors will be recertified annually. nformation system requires callback capability with re-authenticatior quire the vendor to log-on, the vendor should be assigned a User ID and logged. User IDs assigned to vendors will be recertified annually

ASSESSMENT PROCEDURE: AC-17(CMS-	4).1	
Assessment Objective	·	
	cryptography to protect the confidentiality and integrity of remote access sessions.	
Assessment Methods And Objects		
	addressing remote access to the information system; list of information system accounts	s; information system configuration settings and associated
	rds; other relevant documents or records to determine if e-authentication is implemente	
	ote access authorization, monitoring, and control responsibilities to determine if the info	ormation system implements e-authentication. If so, refer to ARS
Appendix A for e-Authentication standards.		
AC-17(FIS-1) – Enhancement (Low)		
Control		
Remote access phone numbers are not publis	shed and are periodically changed.	
Applicability: All	References: FISCAM: TAC-3.2.E.2.2	Related Controls:
ASSESSMENT PROCEDURE: AC-17(FIS-1)).1	
Assessment Objective		
	ically, remote access phone numbers and those phone numbers are not published.	
Assessment Methods And Objects	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Examine: Documentation showing changes to	o dial-in numbers.	
Examine: Entity's telephone directory to verify		
Examine: Pertinent policies and procedures.		
Interview: Remote access users.		
	(1)	
AC-18 – Wireless Access Restrictions Control		red in writing by the CMS CIO or his/ber designated
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s	shall be secured through the use of approved encryption controls
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion	shall be secured through the use of approved encryption controls n detection and prevention.
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s	shall be secured through the use of approved encryption controls
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion	shall be secured through the use of approved encryption controls n detection and prevention.
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion	shall be secured through the use of approved encryption controls n detection and prevention.
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if:	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18	shall be secured through the use of approved encryption controls n detection and prevention.
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18	shall be secured through the use of approved encryption controls n detection and prevention.
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and	shall be secured through the use of approved encryption controls n detection and prevention.
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and	shall be secured through the use of approved encryption controls n detection and prevention.
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist Assessment Methods And Objects Examine: Access control policy; procedures a	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and tent with NIST SP 800-48 and 800-97. addressing wireless implementation and usage (including restrictions); NIST SP 800-48	hall be secured through the use of approved encryption control n detection and prevention. Related Controls:
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist Assessment Methods And Objects Examine: Access control policy; procedures a monitoring, and control; information system au	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and tent with NIST SP 800-48 and 800-97. addressing wireless implementation and usage (including restrictions); NIST SP 800-48 udit records; other relevant documents or records.	n detection and prevention. Related Controls:
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist Assessment Methods And Objects Examine: Access control policy; procedures a monitoring, and control; information system au Test: Wireless access usage and restrictions.	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and tent with NIST SP 800-48 and 800-97. addressing wireless implementation and usage (including restrictions); NIST SP 800-48 udit records; other relevant documents or records.	hall be secured through the use of approved encryption control n detection and prevention. Related Controls:
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist Assessment Methods And Objects Examine: Access control policy; procedures a monitoring, and control; information system au Test: Wireless access usage and restrictions. AC-18(0) – Enhancement (Low)	nto CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and tent with NIST SP 800-48 and 800-97. addressing wireless implementation and usage (including restrictions); NIST SP 800-48 udit records; other relevant documents or records.	hall be secured through the use of approved encryption control n detection and prevention. Related Controls:
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist Assessment Methods And Objects Examine: Access control policy; procedures a monitoring, and control; information system au Test: Wireless access usage and restrictions. AC-18(0) – Enhancement (Low) Control	to CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and tent with NIST SP 800-48 and 800-97. addressing wireless implementation and usage (including restrictions); NIST SP 800-48 udit records; other relevant documents or records. (Optional)	n detection and prevention. Related Controls:
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist Assessment Methods And Objects Examine: Access control policy; procedures a monitoring, and control; information system au Test: Wireless access usage and restrictions. AC-18(0) – Enhancement (Low) Control CMS policy prohibits the use of wireless access	to CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and tent with NIST SP 800-48 and 800-97. addressing wireless implementation and usage (including restrictions); NIST SP 800-48 udit records; other relevant documents or records. (Optional)	And 800-97; activities related to wireless authorization,
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization establishes usage restriction (iii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist Assessment Methods And Objects Examine: Access control policy; procedures a monitoring, and control; information system au Test: Wireless access usage and restrictions. AC-18(0) – Enhancement (Low) Control CMS policy prohibits the use of wireless access Applicability: All	to CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and tent with NIST SP 800-48 and 800-97. addressing wireless implementation and usage (including restrictions); NIST SP 800-48 udit records; other relevant documents or records. (Optional)	n detection and prevention. Related Controls:
Control Installation of wireless access points (WAP) in representative. Authorized WAP devices and Guidance NIST SP 800-48 and 800-97 provide guidance Applicability: All ASSESSMENT PROCEDURE: AC-18.1 Assessment Objective Determine if: (i) the organization establishes usage restriction (ii) the organization authorizes, monitors, and (iii) the wireless access restrictions are consist Assessment Methods And Objects Examine: Access control policy; procedures a monitoring, and control; information system au Test: Wireless access usage and restrictions. AC-18(0) – Enhancement (Low) Control CMS policy prohibits the use of wireless access	to CMS information systems and networks shall be prohibited unless explicitly authoriz wireless access shall be monitored on a regular basis, and wireless communications s e on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion References: ARS: AC-18; NIST 800-53/53A: AC-18; PISP: 4.1.18 ons and implementation guidance for wireless technologies; controls wireless access to the information system; and tent with NIST SP 800-48 and 800-97. addressing wireless implementation and usage (including restrictions); NIST SP 800-48 udit records; other relevant documents or records. (Optional)	And 800-97; activities related to wireless authorization,

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST SP 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records.

AC-18(DIR-1) – Enhancement (Low)

Control

If wireless access is explicitly approved, wireless devices, service set identifier broadcasting is disabled and the following wireless access controls are implemented:

(a) encryption protection is enabled;

(b) access points are placed in secure areas;

(c) access points are shut down when not in use (i.e., nights, weekends);

(d) a firewall is implemented between the wireless network and the wired infrastructure:

(e) MAC address authentication is utilized;

(f) static IP addresses, not DHCP, is utilized;

(g) personal firewalls are utilized on all wireless clients;

(h) file sharing is disabled on all wireless clients:

(i) Intrusion detection agents are deployed on the wireless side of the firewall: and

(i) wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

References:

Applicability: All

ASSESSMENT PROCEDURE: AC-18(DIR-1).1

Assessment Objective

Determine if the organization establishes wireless policies and strict procedures that control access to the wireless LAN and separates/restricts the wireless LAN from the wireless and strict procedures that control access to the wireless LAN and separates/restricts the wireless LAN from the wireless and strict procedures that control access to the wireless LAN and separates/restricts the wireless LAN from the wireless and strict procedures that control access to the wireless LAN and separates/restricts the wireless LAN from the wireless and strict procedures that control access to the wireless LAN and separates/restricts the wireless LAN from the wireless that control access to the wireless LAN and separates/restricts the wireless that control access to the wireless LAN and separates/restricts the wireless that control access to the wireless that control access that control access to the wireless that control access to the wireless that control access tha **Assessment Methods And Objects**

Examine: Access control procedures for continuous wireless intrusion monitoring of approved and operational wireless systems.

Interview: Staff personnel who review the wireless LAN records know what to look for in the data for an unauthorized intrusion, and the staff knows the reporting procedures when an unauthorized intrusion is detected.

AC-19 – Access Control for Portable and Mobile Devices (Low)

Control

The connection of portable and mobile devices (e.g., notebook computers, personal digital assistants (PDA), cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems and networks shall be prohibited unless explicitly authorized, in writing, by the CIO or his/her designated representative. Prior to connecting portable and mobile devices to CMS information systems and networks, such devices shall be configured to comply with CMS IS policies and procedures. The storage and transmission of CMS sensitive information on portable and mobile information devices shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware. The activities and controls shall be commensurate with the system security level of the information.

Guidance

Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family.

Applicability: All	References: ARS: AC-19; IRS-1075: 4.6#1; NIST 800-53/53A: AC-19; PISP: 4.1.19	Related Controls: MP-4, MP-5
ASSESSMENT PROCEDURE: AC-19.1		

Assessment Objective

Determine if:

(i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices:

- (ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and
- (iii) the organization authorizes, monitors, and controls device access to organizational information systems.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (Optional)

Interview: Organizational personnel who use portable and mobile devices to access the information system. (Optional)

Related Controls:

	cess control policy for portable and mobile devices.(Optional)	
AC-20 – Use of External Information Sys	stems (Low)	
Control		
External information systems, including, but not	limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal di available in hotels or airports shall not be used to store, access, transmit, or process CMS sensitive inf	
Strict terms and conditions shall be established 4.1.20.1. The types of applications that can be a 4.1.20.2. The maximum FIPS 199 security categorial	for the use of external information systems. The terms and conditions shall address, at a minimum: accessed from external information systems; gory of information that can be processed, stored, and transmitted; ation system will be prevented from accessing federal information; /PN) and firewall technologies; /ulnerabilities of wireless technologies; I security controls; on software; and	
organization typically has no direct control over limited to, personally owned information systems or public facilities (e.g., hotels, convention cente owned by, operated by, or under the direct contr Authorized individuals include organizational per external information systems to access organiza	rsonnel, contractors, or any other individuals with authorized access to the organizational information systems and information that are intended for public access (e.g., individuals access)	al information systems include, but are not ommunications devices resident in commercia d federal information systems that are not ystem. This control does not apply to the use o ing federal information through public interface
	anization establishes terms and conditions for the use of external information systems in accordance wi as a minimum; (i) the types of applications that can be accessed on the organizational information syste rmation that can be processed, stored, and transmitted on the external information system.	
the maximum FIPS 199 security category of info	as a minimum; (i) the types of applications that can be accessed on the organizational information syste	
the maximum FIPS 199 security category of info pplicability: All ASSESSMENT PROCEDURE: AC-20.1	as a minimum; (i) the types of applications that can be accessed on the organizational information system rmation that can be processed, stored, and transmitted on the external information system. References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP:	m from the external information system; and (
the maximum FIPS 199 security category of info Applicability: All ASSESSMENT PROCEDURE: AC-20.1 Assessment Objective Determine if: (i) the organization defines the types of applicati (ii) the organization defines the maximum FIPS (iii) the organization establishes terms and cond	as a minimum; (i) the types of applications that can be accessed on the organizational information system rmation that can be processed, stored, and transmitted on the external information system. References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP:	erm from the external information system; and (
the maximum FIPS 199 security category of info Applicability: All ASSESSMENT PROCEDURE: AC-20.1 Assessment Objective Determine if: (i) the organization defines the types of applicati (ii) the organization defines the maximum FIPS (iii) the organization establishes terms and cond accessed on the organizational information system.	as a minimum; (i) the types of applications that can be accessed on the organizational information system formation that can be processed, stored, and transmitted on the external information system. References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20 ons that can be accessed from the external information system; 199 security category of information that can be processed, stored, and transmitted on the external information system to itions for authorized individuals to access the information system from an external information system to	erm from the external information system; and (
the maximum FIPS 199 security category of info Applicability: All ASSESSMENT PROCEDURE: AC-20.1 Assessment Objective Determine if: (i) the organization defines the types of applicati (ii) the organization defines the maximum FIPS of (iii) the organization establishes terms and cond accessed on the organizational information system. Assessment Methods And Objects Examine: Access control policy; procedures add external information systems; maximum FIPS 19 associated documentation; other relevant docum	as a minimum; (i) the types of applications that can be accessed on the organizational information system mation that can be processed, stored, and transmitted on the external information system. References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20 ons that can be accessed from the external information system; 199 security category of information that can be processed, stored, and transmitted on the external information system the itions for authorized individuals to access the information system from an external information system the em from the external information system and the maximum FIPS 199 security category of information the dressing the use of external information systems; external information systems terms and conditions; lis 29 impact level for information processed, stored, or transmitted on external information systems; inform- nents or records.	Related Controls:
the maximum FIPS 199 security category of info applicability: All SSESSMENT PROCEDURE: AC-20.1 Assessment Objective Determine if: (i) the organization defines the types of applicati (ii) the organization defines the maximum FIPS (iii) the organization establishes terms and cond accessed on the organizational information syste on the external information system. Assessment Methods And Objects Examine: Access control policy; procedures adde external information systems; maximum FIPS 19 associated documentation; other relevant documentation; other rele	as a minimum; (i) the types of applications that can be accessed on the organizational information system mation that can be processed, stored, and transmitted on the external information system. References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20 ons that can be accessed from the external information system; 199 security category of information that can be processed, stored, and transmitted on the external info itions for authorized individuals to access the information system from an external information system the em from the external information system and the maximum FIPS 199 security category of information the dressing the use of external information systems; external information systems terms and conditions; lis 99 impact level for information processed, stored, or transmitted on external information systems; inform	Related Controls:
the maximum FIPS 199 security category of info Applicability: All ASSESSMENT PROCEDURE: AC-20.1 Assessment Objective Determine if: (i) the organization defines the types of applicati (ii) the organization defines the maximum FIPS (iii) the organization establishes terms and cond accessed on the organizational information syste on the external information system. Assessment Methods And Objects Examine: Access control policy; procedures add external information systems; maximum FIPS 19 associated documentation; other relevant docum Interview: Organizational personnel who use ex AC-20(CMS-1) – Enhancement (Low)	as a minimum; (i) the types of applications that can be accessed on the organizational information system mation that can be processed, stored, and transmitted on the external information system. References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20 ons that can be accessed from the external information system; 199 security category of information that can be processed, stored, and transmitted on the external information system the itions for authorized individuals to access the information system from an external information system the em from the external information system and the maximum FIPS 199 security category of information the dressing the use of external information systems; external information systems terms and conditions; lis 29 impact level for information processed, stored, or transmitted on external information systems; inform- nents or records.	ern from the external information system; and (Related Controls: ermation system; and hat include the types of applications that can be hat can be processed, stored, and transmitted st of types of applications accessible from
the maximum FIPS 199 security category of info Applicability: All ASSESSMENT PROCEDURE: AC-20.1 Assessment Objective Determine if: (i) the organization defines the types of applicati (ii) the organization defines the maximum FIPS (iii) the organization establishes terms and cond accessed on the organizational information syste on the external information system. Assessment Methods And Objects Examine: Access control policy; procedures add external information systems; maximum FIPS 19 associated documentation; other relevant docum Interview: Organizational personnel who use ex AC-20(CMS-1) – Enhancement (Low) Control Instruct all personnel working from home to impl	as a minimum; (i) the types of applications that can be accessed on the organizational information system mation that can be processed, stored, and transmitted on the external information system. References: ARS: AC-20; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1; NIST 800-53/53A: AC-20; PISP: 4.1.20 ons that can be accessed from the external information system; 199 security category of information that can be processed, stored, and transmitted on the external information system the itions for authorized individuals to access the information system from an external information system the em from the external information system and the maximum FIPS 199 security category of information the dressing the use of external information systems; external information systems terms and conditions; lis 29 impact level for information processed, stored, or transmitted on external information systems; inform- nents or records.	em from the external information system; and (Related Controls: armation system; and hat include the types of applications that can be processed, stored, and transmitted st of types of applications accessible from nation system configuration settings and I firewalls. Limit remote access only to

ASSESSMENT PROCEDURE: AC-20(CMS-1).1

Assessment Objective

Determine if the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

Interview: Organizational personnel who use external information systems to access the information system to determine if the organization instructs all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Remote access must be limited only to information resources required by home users to complete job duties. Any government-owned equipment must be used only for business purposes by authorized employees.

AC-CMS-1 – System Boot Access (Low)

Control

System boot access shall be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by the CIO or his/her designated representative. The number of users who can alter or perform non-standard boots of systems and/or components of the information system shall be limited and justification / approval for such access shall be controlled, documented, and monitored.

Guidance

When a person has unrestrained physical access to any computing system or network device the person has control of the equipment.

If the person does not have the capability to locally access the information system's data though the boot process this can assist in protecting the data from loss or unauthorized access to the data. Note: Even though the system root access may be protected by privilege access controls a miss configured system can allow the system to reboot and thus allowing a boot / access from unauthorized media. An example of this is a LINUX system, not configured correctly, when CONT+ALT+DEL is issued from the keyboard the equipment will re-boot automatically.

Applicability: All	References: ARS: AC-CMS-1; PISP: 4.1.21	Related Controls:
ASSESSMENT PROCEDURE:	AC-CMS-1.1	
Assessment Objective		
Determine if the organization as	ssesses the need for system boot access and if necessary controls, documents and monito	ors the continued need for system boot access.
Assessment Methods And Objects		
Examine: System boot access	documentation to determine that there is or is not a need for boot access.	

Interview: Organizational personnel to determine that there is or is not a need for system boot access.

AC-CMS-1(CMS-1) – Enhancement (Low)

Control

If not explicitly required, boot access to removable media drives is disabled.

Applicability: All	References: ARS: AC-CMS-1(CMS-1)	Related Controls:

ASSESSMENT PROCEDURE: AC-CMS-1(CMS-1).1

Assessment Objective

Determine if the organization evaluates the need for system boot access by removable media drives.

Assessment Methods And Objects

Examine: System boot access documentation to determine that, if not explicitly required, boot access to removable media drives is disabled.

Interview: Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled.

AC-CMS-1(CMS-2) – Enhancement (Low)		
Control		
System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).		
Applicability: All	References: ARS: AC-CMS-1(CMS-2)	Related Controls: IA-5

ASSESSMENT PROCEDURE: AC-CMS-1(CMS-2).1

Assessment Objective

Determine if the organization controls access to the system BIOS when unauthorized personnel may be in physical proximity to the system.

Assessment Methods And Objects

Examine: System BIOS documentation to determine if System BIOS settings are locked and BIOS access is protected by password (see IA-5, Authenticator Management).

Interview: Organizational personnel to determine that, if not explicitly required, boot access to removable media drives is disabled.

Awareness and Training (AT) – Operational

AT-1 – Security Awareness and Training Policy and Procedures (Low)

Control

An IS AT program shall be developed, documented, and implemented effectively for all personnel, including contractors and any other users of CMS information and information systems. The IS AT program shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-50. AT shall be completed by all personnel prior to granting authorization to access to CMS information, information systems, and networks.

Guidance

The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-16 and 800-50 provide guidance on security awareness and training. NIST SP 800-12 provides guidance on security policies and procedures.

	1; PISP: 4.2.1	
Applicability: All	References: ARS: AT-1; FISCAM: TSP-4.2.2; IRS-1075: 5.6.2.7#1.1-2, 6.1#1; NIST 800-53/53A: AT-	Related Controls:

ASSESSMENT PROCEDURE: AT-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security awareness and training policy and procedures;

(ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review security awareness and training policy and procedures; and

(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.

Interview: Organizational personnel with security awareness and training responsibilities.(Optional)

ASSESSMENT PROCEDURE: AT-1.2

Assessment Objective

Determine if:

(i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with security awareness and training responsibilities.(Optional)

AT-2 – Security Awareness (Low)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that CMS information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment. The IS AT program shall be consistent with 5 CFR Part 930 (http://opm.gov/fedregis/2004/69-061404-32835-a.pdf) and the guidance provided in NIST SP 800-50.

Guidance

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST SP 800-50.

Applicability: All	References: ARS: AT-2; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3; NIST 800-53/53A: AT-2; PISP: 4.2.2	Related Controls:
ASSESSMENT PROCEDURE: AT-2.1	-	

ASSESSMENT PROCEDORE. AT

Assessment Objective

(i) the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes; (ii) the security awareness training is consistent with applicable regulations and NIST SP 800-50;				
	(ii) the security awareness training is consistent with applicable regulations and NIST SP 800-50; (iii) the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access;			
(iv) the organization defines the frequency of ref				
	(v) the organization defines the nequency of refresher security awareness training, and (v) the organization provides refresher security awareness training in accordance with organization-defined frequency, at least annually.			
Assessment Methods And Objects				
Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan; other relevant documents or records.				
	the general information system user community.(Optional)			
AT-2(0) – Enhancement (Low)				
Control				
changes; and every 365 days thereafter.	s and senior executives) receive basic information security awareness training prior to accessing any sys			
Applicability: All	References: ARS: AT-2(0); FISCAM: TSP-3.3.1; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3, 6.2#1.1-2, 6.2#1.4, 6.2#2.1; NIST 800-53/53A: AT-2; PISP: 4.2.2	Related Controls:		
ASSESSMENT PROCEDURE: AT-2(0).1				
Assessment Objective				
o 1	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ving enhancement to the baseline control.		
Assessment Methods And Objects				
	y; procedures addressing security awareness training implementation; NIST SP 800-50; appropriate cod materials; information system security plan (for organization-defined frequency of refresher security awar			
records.	materials, mormation system security plan (for organization-defined nequency of refresher security awar	eness training), other relevant documents of		
AT-2(CMS-1) – Enhancement (Low)				
Control				
Establish a program to promote continuing awar	eness of information security issues and threats.			
Applicability: All	References: ARS: AT-2(CMS-1); HIPAA: 164.308(a)(5)(ii)(A); IRS-1075: 5.6.2.7#1.3	Related Controls:		
ASSESSMENT PROCEDURE: AT-2(CMS-1).1				
Assessment Objective				
Determine if the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes.				
Assessment Methods And Objects				
Examine: Security awareness and training policy and procedures; other relevant documents or records to determine that a program to promote continuing awareness of information security issues and threats has been established.				
Interview: Organizational personnel with security awareness and training responsibilities to determine that a program to promote continuing awareness of information security issues and threats has been established.				
AT-3 – Security Training (Low)				
Control				
	positions and/or roles with significant information system security responsibilities during the system deve			
	ilities shall receive appropriate security training consistent with NIST SP 800-16 and NIST SP 800-50. C			
shall be determined based upon the information systems to which personnel have authorized access. The employee shall acknowledge having received the security and awareness training either in				
writing or electronically as part of the training course completion.				
	ntent of security training based on the specific requirements of the organization and the information syste	ms to which personnel have authorized		
	stem managers, system and network administrators, and other personnel having access to system-level			
perform their assigned duties. The organization's	s security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.			
SP 800-50.				
Applicability: All	References: ARS: AT-3; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	Related Controls:		
Rev. 9	Page 23 of 127	BPSSM Appendix A. Attachment 3		

ASSESSMENT PROCEDURE: AT-3.1

Assessment Objective

Determine if:

(i) the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities;

(ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes;

(iii) the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security;

(iv) the security training is consistent with applicable regulations and NIST SP 800-50;

(v) the organization defines the frequency of refresher security training; and

(vi) the organization provides refresher security training in accordance with organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan; other relevant documents or records.

Interview: Organizational personnel with significant information system security responsibilities.(Optional)

AT-3(0) – Enhancement (Low)

Control

Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to CMS networks, systems, and/or applications; when required by system changes; and refresher training every 365 days thereafter.

Applicability: All	References: ARS: AT-3(0); FISCAM: TSP-3.3.1; IRS-1075: 5.6.2.7#1.4; NIST 800-53/53A: AT-3; PISP: 4.2.3	Related Controls:
ASSESSMENT DROCEDURE, AT 2(0) 4		

ASSESSMENT PROCEDURE: AT-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; NIST SP 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan (for organization-defined frequency of refresher security training); other relevant documents or records.

AT-4 – Security Training Records (Low)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that individual IS training activities, including basic security awareness training and specific information system security training, are properly documented and monitored.

Guidance

Procedures and training implementation should:

(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:

(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.

(2) Executives must receive training in information security basics and policy level training in security planning and management.

(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.

(4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.

(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.

(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.

(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process. (d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	References: ARS: AT-4; FISCAM: TSP-4.2.3; IRS-1075: 6.2#1.3; NIST 800-53/53A: AT-4; PISP: 4.2.4	Related Controls:			
ASSESSMENT PROCEDURE: AT-4.1					
Assessment Objective					
Determine if the organization monitors and docu	Determine if the organization monitors and documents basic security awareness training and specific information system security training.				
Assessment Methods And Objects					
Examine: Security awareness and training polic	y; procedures addressing security training records; security awareness and training records; other relevant	ant documents or records.			
AT-5 – Contacts with Security Groups a	nd Associations (Low)				
Control					
Contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations shall be encouraged and supported to enable security personnel to stay up to date with the latest recommended security practices, techniques, and technologies; and to share the latest security-related information including threats, vulnerabilities, and incidents.					
Guidance					
contacts with selected groups and associations v	ing for organizational personnel in an environment of rapid technology changes and dynamic threats, th within the security community. The groups and associations selected are in keeping with the organization incidents related to information systems are consistent with applicable laws, Executive Orders, directives	on's mission requirements. Information sharing			
Applicability: All	References: ARS: AT-5; HSPD 7: H(25); NIST 800-53/53A: AT-5; PISP: 4.2.5	Related Controls:			
ASSESSMENT PROCEDURE: AT-5.1					
Assessment Objective Determine if the organization establishes and ma techniques and technologies and to share securi Assessment Methods And Objects	aintains contact with special interest groups, specialized forums, or professional associations to keep cu ity-related information.	irrent with state-of-the-practice security			

Examine: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records.(Optional)

Audit and Accountability (AU) – Technical

AU-1 – Audit and Accountability Policy and Procedures (Low)			
Control			
	All CMS information systems shall be configured to produce, store, and retain audit records of specific system, application, network, and user activity. Procedures shall be developed to guide the		
implementation and management of audit controls, and shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed			
periodically, and, if necessary, updated.			
Guidance			
The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability			
policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.			
particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. Applicability: All References: ARS: AU-1; IRS-1075: 5.6.3.3#1; NIST 800-53/53A: AU-1; PISP: 4.3.1 Related Controls:			
Applicability: All References: ARS: AU-1; IRS-1075: 5.6.3.3#1; NIST 800-53/53A: AU-1; PISP: 4.3.1 Related Controls:			
Assessment Objective			
Determine if:			
(i) the organization develops and documents aud	it and accountability policy and procedures;		
(ii) the organization disseminates audit and account	intability policy and procedures to appropriate elements within the organization;		
(iii) responsible parties within the organization pe	riodically review audit and accountability policy and procedures; and		
() 0 1	ility policy and procedures when organizational review indicates updates are required.		
Assessment Methods And Objects			
Examine: Audit and accountability policy and pro			
Interview: Organizational personnel with audit an	nd accountability responsibilities.(Optional)		
ASSESSMENT PROCEDURE: AU-1.2			
Assessment Objective			
Determine if:			
	purpose, scope, roles and responsibilities, management commitment, coordination among organizationa		
(ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and			
(iii) the audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant implementations of all associated security controls.			
controls. Assessment Methods And Objects			
Examine: Audit and accountability policy and procedures; other relevant documents or records.			
Interview: Organizational personnel with audit and accountability responsibilities.(Optional)			
AU-2 – Auditable Events (Low)			
Control			
Automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security			
	incidents. The selection of auditable events shall be based upon a risk assessment as to which events require auditing on a continuous basis, and which events require auditing in response to		
specific situations.			
Guidance			
	The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require		
	require auditing in response to specific situations. Audit records can be generated at various levels of a		
	and level of abstraction for audit record generation is a critical aspect of an audit capability and can facilit		
problems. Additionally, the security audit function	is coordinated with the network health and status monitoring function to enhance the mutual support be	etween the two functions by the selection of	
information to be recorded by each function. The	checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of au	ditable events. The organization defines	
	er-the-fact investigations of security incidents. NIST SP 800-92 provides guidance on computer security		
Applicability: All	References: ARS: AU-2; FISCAM: TAC-4.3.4, TSD-3.2.2; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1; NIST 800-53/53A: AU-2; PISP: 4.3.2	Related Controls: AU-4	

ASSESSMENT PROCEDURE: AU-2.1			
ssessment Objective			
Determine if:			
 (i) the organization defines information system auditable events; (ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and 			
	ds for the organization-defined auditable events.		
ssessment Methods And Objects			
	dures addressing auditable events; information system security plan; information system configuration s	attings and appreciated decumentation.	
information system audit records; other relevant		ettings and associated documentation,	
	prmation system auditing of organization-defined auditable events.(Optional)		
U-2(0) – Enhancement (Low)			
Control			
Generate audit records for the following events:			
(a) User account management activities,			
(b) System shutdown,			
(c) System reboot,			
(d) System errors,			
(e) Application shutdown, (f) Application restart,			
(g) Application errors,			
(h) File creation, and			
(i) File deletion.			
pplicability: All	References: ARS: AU-2(0); FISCAM: TAC-2.1.5, TAC-4.1, TSD-3.2.4; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3; NIST 800-53/53A: AU-2; PISP: 4.3.2	Related Controls:	
SSESSMENT PROCEDURE: AU-2(0).1		•	
ssessment Objective			
Determine if the organization meets the requirer	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ying enhancement to the baseline control.	
ssessment Methods And Objects			
Examine: Audit and accountability policy; proce	dures addressing auditable events; information system security plan (for list of organization-defined aud	table events); information system	
	ation; information system audit records; other relevant documents or records.		
U-2(CMS-1) – Enhancement (Low)			
ontrol	Second Barray dama dama		
Enable logging for perimeter devices, including f (a) Log packet screening denials originating from			
(b) Packet screening denials originating from tru			
(c) User account management,			
(c) User account management, (d) Modification of packet filters,			
 (c) User account management, (d) Modification of packet filters, (e) Application errors, (f) System shutdown and reboot, and (g) System errors. 			
 (c) User account management, (d) Modification of packet filters, (e) Application errors, (f) System shutdown and reboot, and (g) System errors. 	References: ARS: AU-2(CMS-1); HIPAA: 164.312(b); IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3	Related Controls:	
(c) User account management, (d) Modification of packet filters, (e) Application errors, (f) System shutdown and reboot, and (g) System errors. pplicability: All SSESSMENT PROCEDURE: AU-2(CMS-1).1		Related Controls:	
(c) User account management, (d) Modification of packet filters, (e) Application errors, (f) System shutdown and reboot, and (g) System errors. pplicability: All SSESSMENT PROCEDURE: AU-2(CMS-1).1 ssessment Objective		Related Controls:	
(c) User account management, (d) Modification of packet filters, (e) Application errors, (f) System shutdown and reboot, and (g) System errors. pplicability: All SSESSMENT PROCEDURE: AU-2(CMS-1).1 ssessment Objective Determine if:		Related Controls:	
 (c) User account management, (d) Modification of packet filters, (e) Application errors, (f) System shutdown and reboot, and (g) System errors. pplicability: All SESSMENT PROCEDURE: AU-2(CMS-1).1 ssessment Objective Determine if: (i) the organization defines information system a 	uditable events;	Related Controls:	
 (c) User account management, (d) Modification of packet filters, (e) Application errors, (f) System shutdown and reboot, and (g) System errors. oplicability: All SSESSMENT PROCEDURE: AU-2(CMS-1).1 sessment Objective Determine if: (i) the organization defines information system a (ii) the organization-defined auditable events are 		Related Controls:	

Assessment Methods And Objects

Assessment Methods And Objects	
	dures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system
	ation; information system audit records; other relevant documents or records to determine if logging-on is enabled for perimeter devices, including
firewalls and routers. This logging will capture the	
(a) Log packet screening denials originating from	
(b) packet screening denials originating from tru	sted networks,
(c) user account management,(d) modification of proxy services,	
(e) application errors,	
(f) system shutdown and reboot,	
(g) system errors,	
(h) modification of proxy services, and	
(i) modification of packet filters.	
Interview: Organizational personnel with audit a	nd accountability responsibilities to determine if logging-on is enabled for perimeter devices, including firewalls and routers. This logging will capture
the following information:	
(a) Log packet screening denials originating from	
(b) packet screening denials originating from tru	sted networks,
(c) user account management,	
(d) modification of proxy services,	
(e) application errors,	
(f) system shutdown and reboot, (g) system errors,	
(b) modification of proxy services, and	
(i) modification of packet filters.	
AU-2(CMS-2) – Enhancement (Low)	
Control	
Control	audit administrator activities
Verify that proper logging is enabled in order to	
Verify that proper logging is enabled in order to a Applicability: All	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2). Assessment Objective	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls:
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events. Image: Control of the organization defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events. Image: Control of the organization defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities.	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with account	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 – Content of Audit Records (Low)	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 – Content of Audit Records (Low) Control	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events. udit records for the organization-defined auditable events. dures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system ation; information system audit records; other relevant documents or records to determine if proper logging is enabled in order to audit administrator activities. at audit and accountability responsibilities to determine if proper logging is enabled in order to audit administrator activities.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 – Content of Audit Records (Low) Control Automated mechanisms shall be established to	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 – Content of Audit Records (Low) Control Automated mechanisms shall be established to	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events. udit records for the organization-defined auditable events. dures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system ation; information system audit records to determine if proper logging is enabled in order to audit administrator to audit administrator activities. audit and accountability responsibilities to determine if proper logging is enabled in order to audit administrator activities. brovide the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 - Content of Audit Records (Low) Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit record	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 - Content of Audit Records (Low) Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit record	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 - Content of Audit Records (Low) Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit record	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 - Content of Audit Records (Low) Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit records occurred; (iii) type of event; (iv) user/subject ident Applicability: All	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 – Content of Audit Records (Low) Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit records occurred; (iii) type of event; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable of the source occurred; (iv) user/subject identified to a social stable occurred; (iv) user/subject identified to a s	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.
Verify that proper logging is enabled in order to a Applicability: All ASSESSMENT PROCEDURE: AU-2(CMS-2).1 Assessment Objective Determine if the information system generates a Assessment Methods And Objects Examine: Audit and accountability policy; proce configuration settings and associated document activities. Interview: Organizational personnel with accound AU-3 - Content of Audit Records (Low) Control Automated mechanisms shall be established to occurred, when the events occurred, the source Guidance Audit record content includes, for most audit records occurred; (iii) type of event; (iv) user/subject ident Applicability: All	References: ARS: AU-2(CMS-2); FISCAM: TAC-2.1.5, TSS-2.1.4; IRS-1075: 5.6.3.3#2.1, 5.6.3.3#3 Related Controls: udit records for the organization-defined auditable events.

Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Assessment Methods And Object		motion quatern qualit recorded information quatern incident
reports; other relevant documents of	v policy; procedures addressing content of audit records; list of organization-defined auditable events; inform or records	mation system audit records, information system incident
	elementing information system auditing of auditable events.(Optional)	
AU-4 – Audit Storage Capacity		
Control	y (2007)	
	system storage capacity shall be allocated for audit records, and information systems shall be configured to	to reduce the likelihood of audit records exceeding such
Guidance		
	nt audit storage capacity, taking into account the auditing to be performed and the online audit processing re-	requirements
Applicability: All	References: ARS: AU-4; IRS-1075: 5.6.3.3#4; NIST 800-53/53A: AU-4; PISP: 4.3.4	Related Controls: AU-2, AU-5, AU-6, AU- 7, SI-4
ASSESSMENT PROCEDURE: AU	-4.1	
Assessment Objective		
Determine if:		
	ecord storage capacity for the information system components that generate audit records; and	
., .	formation system configuration settings to reduce the likelihood of the audit record storage capacity being e	exceeded.
Assessment Methods And Object		
	/ policy; procedures addressing audit storage capacity; information system design documentation; organiza	ation-defined audit record storage capacity for information
	idit records; list of organization-defined auditable events; information system configuration settings and ass	
	u u u u u u u u u u	
other relevant documents or record		
other relevant documents or record	ds.	
other relevant documents or record AU-5 – Response to Audit Pro	ds.	
other relevant documents or record AU-5 – Response to Audit Pro Control	ds. ocessing Failures (Low)	
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be es	ds. DCESSING Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the	
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be es reached and to take appropriate ad	ds. DCESSING Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the	
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be es reached and to take appropriate ad Guidance	ds. DCESSING Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions.	e event of an audit failure or audit storage capacity being
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for	ds. DCESSING Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. For example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac	e event of an audit failure or audit storage capacity being city being reached or exceeded.
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All	ds. DCESSING Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. For example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5	e event of an audit failure or audit storage capacity being
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU-	ds. DCESSING Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. For example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5	e event of an audit failure or audit storage capacity being city being reached or exceeded.
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective	ds. DCESSING Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. For example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5	e event of an audit failure or audit storage capacity being city being reached or exceeded.
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be es- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if:	ds. DCessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1	e event of an audit failure or audit storage capacity being city being reached or exceeded.
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be es- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions	ds. DCessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 is to be taken in the event of an audit processing failure;	e event of an audit failure or audit storage capacity being city being reached or exceeded.
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines person	ds. DCessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 is to be taken in the event of an audit processing failure; nel to be notified in case of an audit processing failure; and	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines personal (iii) the information system alerts ap	ds. DCessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 a to be taken in the event of an audit processing failure; nel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an a	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines personn (iii) the information system alerts ap Assessment Methods And Object	ds. DCessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 is to be taken in the event of an audit processing failure; nel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an acts	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached.
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines personal (iii) the information system alerts ap Assessment Methods And Object Examine: Audit and accountability	ds. DCessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 a to be taken in the event of an audit processing failure; nel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an a	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached. ntation; information system security plan; information
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines personn (iii) the information system alerts ap Assessment Methods And Object Examine: Audit and accountability system configuration settings and a records.	ds. DCessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capac References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 to be taken in the event of an audit processing failure; nel to be notified in case of an audit processing failure; and uppropriate organizational officials and takes any additional organization-defined actions in the event of an a ets r policy; procedures addressing response to audit processing failures; information system design document	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached. ntation; information system security plan; information
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be es- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines person (iii) the information system alerts ap Assessment Methods And Object Examine: Audit and accountability system configuration settings and a records. Test: Automated mechanisms impl	ds. Dcessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capace References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 a to be taken in the event of an audit processing failure; nel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an a ts r policy; procedures addressing response to audit processing failures; information system design document associated documentation; list of personnel to be notified in case of an audit processing failure; information	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached. ntation; information system security plan; information
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines personn (iii) the information system alerts ap Assessment Methods And Object Examine: Audit and accountability system configuration settings and a records.	ds. Dcessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capace References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 a to be taken in the event of an audit processing failure; nel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an a ts r policy; procedures addressing response to audit processing failures; information system design document associated documentation; list of personnel to be notified in case of an audit processing failure; information	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached. ntation; information system security plan; information
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines personal (iii) the information system alerts ap Assessment Methods And Object Examine: Audit and accountability system configuration settings and a records. Test: Automated mechanisms impl AU-5(0) – Enhancement (Low) Control	ds. Dcessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capace References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 a to be taken in the event of an audit processing failure; nel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an a ts r policy; procedures addressing response to audit processing failures; information system design document associated documentation; list of personnel to be notified in case of an audit processing failure; information	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached. ntation; information system security plan; information
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be es- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines person (iii) the information system alerts an Assessment Methods And Object Examine: Audit and accountability system configuration settings and a records. Test: Automated mechanisms impl AU-5(0) – Enhancement (Low) Control Alert appropriate officials and take (a) Shutdown the information system	ds. Decessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capace References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 a to be taken in the event of an audit processing failure; nnel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an acts / policy; procedures addressing response to audit processing failures; information system design document associated documentation; list of personnel to be notified in case of an audit processing failure; information plementing information system response to audit processing failures.(Optional) the following actions in response to an audit failure or audit storage capacity issue: em,	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached. ntation; information system security plan; information
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be es- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines person (iii) the information system alerts and Assessment Methods And Object Examine: Audit and accountability system configuration settings and a records. Test: Automated mechanisms impl AU-5(0) – Enhancement (Low) Control Alert appropriate officials and take i (a) Shutdown the information system (b) Stop generating audit records, c	ds. Decessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capace References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 e to be taken in the event of an audit processing failure; nnel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an action (policy; procedures addressing response to audit processing failures; information system design document associated documentation; list of personnel to be notified in case of an audit processing failure; information plementing information system response to audit processing failures.(Optional) the following actions in response to an audit failure or audit storage capacity issue: em, or	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached. ntation; information system security plan; information
other relevant documents or record AU-5 – Response to Audit Pro Control Automated mechanisms shall be ex- reached and to take appropriate ad Guidance Audit processing failures include, for Applicability: All ASSESSMENT PROCEDURE: AU- Assessment Objective Determine if: (i) the organization defines actions (ii) the organization defines personn (iii) the information system alerts ap Assessment Methods And Object Examine: Audit and accountability system configuration settings and a records. Test: Automated mechanisms impl AU-5(0) – Enhancement (Low) Control Alert appropriate officials and take i (a) Shutdown the information system (b) Stop generating audit records, c	ds. Decessing Failures (Low) established which provide the capability to generate information system alerts for appropriate officials in the dditional actions. for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capace References: ARS: AU-5; NIST 800-53/53A: AU-5; PISP: 4.3.5 I-5.1 a to be taken in the event of an audit processing failure; nnel to be notified in case of an audit processing failure; and appropriate organizational officials and takes any additional organization-defined actions in the event of an acts / policy; procedures addressing response to audit processing failures; information system design document associated documentation; list of personnel to be notified in case of an audit processing failure; information plementing information system response to audit processing failures.(Optional) the following actions in response to an audit failure or audit storage capacity issue: em,	e event of an audit failure or audit storage capacity being city being reached or exceeded. Related Controls: AU-4 audit failure or audit storage capacity being reached. ntation; information system security plan; information

ASSESSMENT PROCEDURE: AU-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for list of actions to be taken by the information system in case of an audit processing failure); information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

AU-6 – Audit Monitoring, Analysis, and Reporting (Low)

Control

Information system audit records shall be reviewed and analyzed regularly to identify and detect unauthorized, inappropriate, unusual, and/or suspicious activity. Such activity shall be investigated and reported to appropriate officials, in accordance with current CMS Procedures.

Guidance

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Applicability: All	References: ARS: AU-6; FISCAM: TAC-2.1.5, TAC-4.3.1, TAN-2.1.8; HIPAA: 164.308(a)(1)(ii)(D),	Related Controls: AU-4, IR-4
	164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1; NIST 800-53/53A: AU-6; PISP: 4.3.6	

ASSESSMENT PROCEDURE: AU-6.1

Assessment Objective

Determine if:

(i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity;

(ii) the organization investigates suspicious activity or suspected violations;

(iii) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and

(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records.(Optional)

Test: Information system audit monitoring, analysis, and reporting capability.(Optional)

ASSESSMENT PROCEDURE: AU-6.2

Assessment Objective

Determine if the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.(Optional) **Interview:** Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities.(Optional)

AU-6(CMS-1) – Enhancement (Low)

Control

Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment.

Applicability: All	References: ARS: AU-6(CMS-1); FISCAM: TAC-4.2	Related Controls:
ACCECCMENT DROCEDURE: ALL C/CMC 4) 4		

ASSESSMENT PROCEDURE: AU-6(CMS-1).1

Assessment Objective

Determine if:

(i) the organization regularly reviews / analyzes audit records for indications of inappropriate or unusual activity;

(ii) the organization investigates suspicious activity or suspected violations;

(iii) the organization reports findings of inappropriate/usual activities, suspicious behavior, or suspected violations to appropriate officials; and

(iv) the organization takes necessary actions in response to the reviews/analyses of audit records.

Assessment Methods And Objects Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records: other relevant documents or records for initialization sequences. log-ons and errors: system processes and performance: and system resources utilization to determine if anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment. Interview: Organizational personnel responsible for audit and accountability to determine if initialization sequences, log-ons and errors; system processes and performance; and system resource utilization are recorded to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical staff review and assessment. AU-6(CMS-2) – Enhancement (Low) Control Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment. Applicability: All References: ARS: AU-6(CMS-2) **Related Controls:** ASSESSMENT PROCEDURE: AU-6(CMS-2).1 **Assessment Objective** Determine if the organization regularly reviews / analyzes audit records for indications of inappropriate or unusual activity. **Assessment Methods And Objects** Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records: other relevant documents or records for initialization sequences, log-ons and errors: system processes and performance; and system resources utilization to determine if network traffic. bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment. Interview: Organizational personnel responsible for audit and accountability to determine if network traffic, bandwidth utilization rates, alert notifications, and border defense devices are reviewed to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical staff review and assessment. AU-6(CMS-3) – Enhancement (Low) Control Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action. Applicability: All References: ARS: AU-6(CMS-3); FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.3, TAC-4.3.4; **Related Controls:** HIPAA: 164.312(b) ASSESSMENT PROCEDURE: AU-6(CMS-3).1 **Assessment Objective** Determine if the organization investigates suspicious activity or suspected violations. **Assessment Methods And Objects** Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records: other relevant documents or records for initialization sequences. log-ons and errors: system processes and performance: and system resources utilization to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action. Interview: Organizational personnel responsible for audit and accountability to determine if the organization investigates suspicious activity or suspected violations on the information system, and reports findings to appropriate officials and takes appropriate action. AU-6(CMS-4) – Enhancement (Low) Control Use automated utilities to review audit records at least once every fourteen (14) days for unusual, unexpected, or suspicious behavior. Applicability: All References: ARS: AU-6(CMS-4); HIPAA: 164.312(b) **Related Controls:** ASSESSMENT PROCEDURE: AU-6(CMS-4).1 **Assessment Objective** Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Assessment Methods And Objects Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or suspicious behavior. Interview: Organizational personnel responsible for audit and accountability to determine if the organization uses automated utilities to review audit records once daily for unusual, unexpected, or

AU-6(CMS-5) – Enhancement (Low)		
Control		
Inspect administrator groups on demand but r	no less than once every thirty (30) days to ensure unauthorized administrator accounts have no	ot been created.
Applicability: All	References: ARS: AU-6(CMS-5); FISCAM: TAC-2.1.5; HIPAA: 164.312(b)	Related Controls:
ASSESSMENT PROCEDURE: AU-6(CMS-5		
Assessment Objective	, ,	
Determine if the organization monitors activitie	es of system administrators.	
Assessment Methods And Objects		
-	cedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records	s of actions taken in response to reviews/analyses of au
	for initialization sequences, log-ons and errors; system processes and performance; and syste	
groups are inspected on demand but at least	once every seven (7) days to ensure unauthorized administrator accounts have not been creat	ited.
Interview: Organizational personnel with audi unauthorized administrator accounts have not	it and accountability responsibilities to determine if administrator groups are inspected on dem t been created.	nand but at least once every seven (7) days to ensure
AU-6(FIS-1) – Enhancement (Low)		
Control		
	lities is reviewed by technical management. Systems programmers' activities are monitored an	nd reviewed. Inappropriate or unusual activity in using
utilities is investigated.		
Applicability: All	References: FISCAM: TSS-2.2.1, TSS-2.2.2, TSS-2.2.3	Related Controls:
ASSESSMENT PROCEDURE: AU-6(FIS-1).	1	
Assessment Objective		
	views system programmers' activities and investigates inappropriate or unusual activities wher	n using privileged system software utilities.
	views system programmers' activities and investigates inappropriate or unusual activities wher	n using privileged system software utilities.
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe	ervising and monitoring of systems programmers' activities.	n using privileged system software utilities.
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev	ervising and monitoring of systems programmers' activities. views.	n using privileged system software utilities.
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev Examine: Documentation supporting these in	ervising and monitoring of systems programmers' activities. views.	n using privileged system software utilities.
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures.	ervising and monitoring of systems programmers' activities. views. nvestigations.	n using privileged system software utilities.
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors	ervising and monitoring of systems programmers' activities. views. nvestigations. to determine their activities related to supervising and monitoring their staff.	n using privileged system software utilities.
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding	ervising and monitoring of systems programmers' activities. views. nvestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage.	n using privileged system software utilities.
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Ge	ervising and monitoring of systems programmers' activities. views. nvestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage.	n using privileged system software utilities.
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Ge Control	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low)	
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Ge Control Automated mechanisms shall be established a	ervising and monitoring of systems programmers' activities. views. nvestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage.	
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Ge Control Automated mechanisms shall be established a generation of appropriate audit reports.	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low)	
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Ge Control Automated mechanisms shall be established a generation of appropriate audit reports. Guidance	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en	
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Ge Control Automated mechanisms shall be established a generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools sup-	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en- upport after-the-fact investigations of security incidents without altering original audit records.	enable human review of audit information and the
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Ge Control Automated mechanisms shall be established a generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools su Applicability: All	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en	
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Go Control Automated mechanisms shall be established generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools su Applicability: All ASSESSMENT PROCEDURE: AU-7.1	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en- upport after-the-fact investigations of security incidents without altering original audit records.	enable human review of audit information and the
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Get Control Automated mechanisms shall be established generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools su Applicability: All ASSESSMENT PROCEDURE: AU-7.1 Assessment Objective	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en- upport after-the-fact investigations of security incidents without altering original audit records. References: ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7	enable human review of audit information and the
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Go Control Automated mechanisms shall be established generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools su Applicability: All ASSESSMENT PROCEDURE: AU-7.1 Assessment Objective Determine if the information system provides a	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en- upport after-the-fact investigations of security incidents without altering original audit records.	enable human review of audit information and the
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the supe Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Ge Control Automated mechanisms shall be established generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools su Applicability: All ASSESSMENT PROCEDURE: AU-7.1 Assessment Objective Determine if the information system provides a	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en- upport after-the-fact investigations of security incidents without altering original audit records. References: ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7 an audit reduction and report generation capability.	enable human review of audit information and the Related Controls: AU-4
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report Go Control Automated mechanisms shall be established generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools su Applicability: All ASSESSMENT PROCEDURE: AU-7.1 Assessment Objective Determine if the information system provides a Examine: Audit and accountability policy; pro	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en- upport after-the-fact investigations of security incidents without altering original audit records. References: ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7 an audit reduction and report generation capability.	enable human review of audit information and the Related Controls: AU-4
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report G Control Automated mechanisms shall be established generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools su Applicability: All ASSESSMENT PROCEDURE: AU-7.1 Assessment Objective Determine if the information system provides a Examine: Audit and accountability policy; pro information system audit records; other releval	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en- upport after-the-fact investigations of security incidents without altering original audit records. References: ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7 an audit reduction and report generation capability. incedures addressing audit reduction and report generation; information system design document ant documents or records.(Optional)	enable human review of audit information and the Related Controls: AU-4
Determine if the organization monitors and rev Assessment Methods And Objects Examine: Documentation supporting the super Examine: Documentation supporting their rev Examine: Documentation supporting these in Examine: Pertinent policies and procedures. Interview: Systems programmer supervisors Interview: Technical management regarding AU-7 – Audit Reduction and Report G Control Automated mechanisms shall be established generation of appropriate audit reports. Guidance Audit reduction, review, and reporting tools su Applicability: All ASSESSMENT PROCEDURE: AU-7.1 Assessment Objective Determine if the information system provides a Examine: Audit and accountability policy; pro information system audit records; other releval	ervising and monitoring of systems programmers' activities. views. ivestigations. to determine their activities related to supervising and monitoring their staff. their reviews of privileged system software and utilities usage. eneration (Low) and supporting procedures shall be developed, documented, and implemented effectively to en- upport after-the-fact investigations of security incidents without altering original audit records. References: ARS: AU-7; FISCAM: TAC-4.3.3; NIST 800-53/53A: AU-7; PISP: 4.3.7 an audit reduction and report generation capability. incedures addressing audit reduction and report generation; information system design document ant documents or records.(Optional) rmation system audit monitoring, analysis, and reporting responsibilities.(Optional)	enable human review of audit information and the Related Controls: AU-4

AU-8 – Time Stamps (Low)	
Control	
Audit records shall employ time stamps for use in audit record generation. Time stamps of audit records shall be generated using internal system clocks	that are synchronized system-wide.
Guidance	
Time stamps (including date and time) of audit records are generated using internal system clocks.	
Applicability: All References: ARS: AU-8; NIST 800-53/53A: AU-8; PISP: 4.3.8	Related Controls:
ASSESSMENT PROCEDURE: AU-8.1	
Assessment Objective	
Determine if the information system provides time stamps for use in audit record generation.	
Assessment Methods And Objects	
Examine: Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system c	configuration settings and associated
documentation; information system audit records; other relevant documents or records.	g
Test: Automated mechanisms implementing time stamp generation.(Optional)	
AU-9 – Protection of Audit Information (Low)	
Control	
Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.	
Guidance	
Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.	
Applicability: All References: ARS: AU-9; NIST 800-53/53A: AU-9; PISP: 4.3.9	Related Controls:
ASSESSMENT PROCEDURE: AU-9.1	
Assessment Objective	
Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion.	
Assessment Methods And Objects	
Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system	m design documentation: information system
configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records.	, , , , , , , , , , , , , , , , , , ,
Test: Automated mechanisms implementing audit information protection.(Optional)	
AU-11 – Audit Record Retention (Low)	
Control	
Audit records shall be retained to provide support for after-the-fact investigations of security incidents, and to meet regulatory and/or CMS information rete	ention requirements. The National Archives
and Records Administration maintains criteria for record retention across many disciplines and information security retention standards shall not be const	
standards.	
Guidance	
The organization retains audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purp	ooses. This includes, for example, retention
and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions (CMS sensitive information	
audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST SP 800-6	1 provides guidance on computer security
incident handling and audit record retention.	Related Controls:
Applicability: All References: NIST 800-53/53A: AU-11 ASSESSMENT PROCEDURE: AU-11.1	Related Controls.
Assessment Objective	
Determine if: (i) the organization defines the retention period for audit records generated by the information system; and	
(ii) the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of	security incidents and to meet regulatory and
organizational information retention requirements.	security mercents and to meet regulatory and
Assessment Methods And Objects	
Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; informatic	on system audit records: other relevant
documents or records.	

Interview: Organizational personnel with information system audit record retention responsibilities. (Optional)

Interview: Organizational personnel with information system audit record retention responsibilities.(Optional)		
AU-11(0) – Enhancement (Low)		
Control		
Retain audit records for ninety (90) days, and archive old audit records. Retain audit record archives for one (1) year.		
Applicability: All	References: ARS: AU-11(0); NIST 800-53/53A: AU-11; PISP: 4.3.11	Related Controls:
ASSESSMENT PROCEDURE: AU-11(0).1		
Assessment Objective		
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.		
Assessment Methods And Objects		
Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with inform	ation system audit record retention responsibilities.(Optional)	

Certification, Accreditation, and Security Assessments (CA) - Management

CA-1 – Certification, Accreditation, and Security Assessments Policies and Procedures (Low)

Control

All General Support Systems (GSSs) (i.e., hardware and related infrastructure) and Major Applications (MAs) (i.e., application code) shall be certified by the Business Owner and accredited by the CMS CIO or his/her designated representative to ensure that the security controls for each GSS or MA mitigate risk to an acceptable level for protecting the confidentiality, integrity, and availability (CIA) of CMS information and information systems. All C&A and security assessment activities shall be conducted in accordance with current CMS Procedures.

Unless there are major changes to a system, re-certification and re-accreditation of GSSs, MAs, and application systems shall be performed every three (3) years. If there are major changes to the GSS, MA, or application system, re-certification and re-accreditation shall be performed whenever the changes occur. Also, re-accreditation and/or re-certification shall be performed upon the completion of the certification / accreditation action lists, in the case of an interim accreditation. Further, the requirements for re-accreditation / re-certification are listed in section 4.4.6, Security Accreditation (CA-6).

If the CMS CIO or his/her designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval shall be granted only by the CMS CIO or his/her designated representative in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The information system shall meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation shall be granted except by the CMS CIO or his/her designated representatives.

As part of the system certification and accreditation (C&A), an independent evaluation based on the system security level may be performed and the results analyzed. Considering the evaluation results from the system testing, IS Risk Assessment (RA), System Security Plan (SSP), independent system tests and evaluations, the Business Owner and System Developer / Maintainer shall certify that the system meets the security requirements to the extent necessary to protect CMS information adequately and meets an acceptable level of risk. Final accreditation shall be made by the CMS CIO or the Designated Accrediting Authority (DAA).

Guidance

The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST SP 800-53 A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security control assessments. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: CA-1; FISCAM: TSP-5.1.2; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075:	Related Controls: CA-6
	5.6.1.4#1.1-2; NIST 800-53/53A: CA-1; PISP: 4.4.1	

ASSESSMENT PROCEDURE: CA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security assessment and certification and accreditation policies and procedures;

(ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review policy and procedures; and

(iv) the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records.

Interview: Organizational personnel with security assessment and certification and accreditation responsibilities.(Optional)

ASSESSMENT PROCEDURE: CA-1.2

Assessment Objective

Determine if:

(i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records. **Interview:** Organizational personnel with security assessment and certification and accreditation responsibilities.(Optional)

CA-2 – Security Assessments (Low)

Control

Routine assessments of all CMS information systems shall be conducted prior to initial operational capability and authorization to operate; prior to each re-authorization to operate; or when a significant change to the information system occurs. Routine assessments of all CMS information systems shall determine if security controls are implemented correctly, are effective in their application, and comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Routine assessments shall be conducted every 365 days, in accordance with NIST SP 800-53 or an acceptable alternative methodology, to monitor the effectiveness of security controls. Findings are subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information system.

OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST SP 800-53 A provides guidance on security control assessments to include reuse of existing assessment results.

Applicability: All	References: ARS: CA-2; FISCAM: TSP-5.1.1; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1; NIST 800-53/53A: CA-2; PISP: 4.4.2	Related Controls: CA-4, CA-6, CA-7, CA- 7(1), SA-11, SI-2
ASSESSMENT PROCEDURE: CA-2.1		

Assessment Objective

Determine if:

(i) the information system is in the inventory of major information systems; and

(ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually.

Assessment Methods And Objects

Examine: Security assessment policy; procedures addressing security assessments; information system security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records.

CA-3 – Information System Connections (Low)

Control

Management shall authorize in writing through the use of system connection agreements all connections to other information systems outside of the accreditation boundary including systems owned and operated by another program, organization, or contractor in compliance with established CMS connection rules and approval processes. The system connections, which are connections between infrastructure components of a system or application, shall be monitored / controlled on an on-going basis.

Guidance

Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST SP 800-47 provides guidance on connecting information systems.

Applicability: All	References: ARS: CA-3; HSPD 7: F(19); NIST 800-53/53A: CA-3; PISP: 4.4.3	Related Controls: SA-9, SC-7
ASSESSMENT PROCEDURE: CA-3.1		

Assessment Objective

Determine if:

(i) the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary);

(ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements;

(iii) the organization monitors/controls the system interconnections on an ongoing basis; and

(iv) information system connection agreements are consistent with NIST SP 800-47.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records.

Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements.(Optional)

CA-3(CMS-1) – Enhancement (Low)

Control

 Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

 Applicability: All
 References: ARS: CA-3(CMS-1); FISCAM: TAC-2.1.3
 Related Controls:

ASSESSMENT PROCEDURE: CA-3(CMS-1).1

Assessment Objective

Determine if the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; NIST SP 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements to determine each system interconnection is recorded in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

CA-4 – Security Certification (Low)

Control

Business owners shall conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification process shall be integrated into and span across the SDLC. In addition, the Business Owner shall review the certification documentation every 365 days, update the documentation where necessary to reflect any changes to the system, and submit a copy of the updated information to the CIO or his/her designated representative.

Guidance

A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST SP 800-53 A provides guidance on security certification.

Applicability: All	References: ARS: CA-4; FISCAM: TSS-2.2.4; HSPD 7: F(19); IRS-1075: 6.3#1.1-2; NIST 800-	Related Controls: CA-2, CA-6, CA-7, SA-
	53/53A: CA-4; PISP: 4.4.4	11, SI-2

ASSESSMENT PROCEDURE: CA-4.1

Assessment Objective

Determine if:

(i) the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and

(ii) the organization employs a security certification process in accordance with OMB policy and NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.

Interview: Organizational personnel with security certification responsibilities.(Optional)

CA-4(CMS-1) – Enhancement (Low)		
Control		
, , ,, , ,, , ,, , ,, , , , , , , , , , , , , , , , , , , ,	n according to the CMS Information Security Risk Assessment (RA) Procedures.	
Applicability: All	References: ARS: CA-4(CMS-1); HSPD 7: G(24)	Related Controls:
ASSESSMENT PROCEDURE: CA-4(CMS-1).		
Assessment Objective		
	access to information system distribution and transmission lines within organizational facilities.	
Assessment Methods And Objects		
	procedures addressing security certification; information system security plan; security assessment plan	
	elevant documents or records to determine the risk and safeguards of the system according to the CMS I	Information Security Risk Assessment (RA)
Procedures are documented.	ty certification responsibilities to determine the risk and safeguards of the system according to the CMS I	nformation Socurity Pick Accordment (PA)
Procedures are documented.		mormation Security Risk Assessment (RA)
CA-5 – Plan of Action and Milestones (F	POA&M) (Low)	
Control		
A POA&M shall be developed, implemented, an	d updated based on the findings from security control assessments, security impact analyses, and contin	nuous monitoring activities. The POA&M shall
	ated corrective actions to repair deficiencies discovered during the security control assessment, and to re	
the information system.		
	and update risk mitigation efforts. Designated personnel shall define and authorize corrective action plan	is, and monitor corrective action progress.
Guidance	and the the second term of the the median of the day of the the section of the the section of the section of the	
	ment in the security accreditation package developed for the authorizing official and is subject to federal based on the findings from security control assessments, security impact analyses, and continuous monit	
quidance contains instructions regarding organi	zational plans of action and milestones. NIST SP 800-37 provides guidance on the security certification a	und accreditation of information systems. NIST
SP 800-30 provides guidance on risk mitigation.		
Applicability: All	References: ARS: CA-5; FISCAM: TSP-5.2; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4; NIST 800-	Related Controls: CA-7
	53/53A: CA-5; PISP: 4.4.5	
ASSESSMENT PROCEDURE: CA-5.1		
Assessment Objective		
Determine if:		
	organization-defined frequency, a plan of action and milestones for the information system; and	
(ii) the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct any deficiencies noted during the assessment of the security		
controls and to reduce or eliminate known vulnerabilities in the information system.		
Assessment Methods And Objects		
Examine: Certification and accreditation policy; procedures addressing plan of action and milestones; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.		
	f action and milestones development and implementation responsibilities.(Optional)	
CA-5(0) – Enhancement (Low)		
Control		
Develop and submit a plan of action and milesto	nes (POA&M) for any documented information system security finding within thirty (30) days of the final i	results for every internal / external audit /
	date the POA&M monthly until all the findings are resolved.	- · · · · · · · · · · · · · · · · · · ·
Applicability: All	References: ARS: CA-5(0); HSPD 7: G(24); NIST 800-53/53A: CA-5; PISP: 4.4.5	Related Controls:
ASSESSMENT PROCEDURE: CA-5(0).1		
Assessment Objective		
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.		
Assessment Methods And Objects		
Examine: Certification and accreditation policy	and procedures; information system security plan (for organization-defined frequency of plan of action an	d milestones updates); security assessment

plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records. Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.(Optional)		
CA-6 – Security Accreditation (Low)		
Control		
is an interim approval to operate, then the autho implemented effectively, and monitored by the a 4.4.6.1. At least every three (3) years; 4.4.6.2. When substantial changes are made to 4.4.6.3. When changes in requirements result in 4.4.6.4. When changes occur to authorizing legis	the need to process data of a higher sensitivity; slation or federal requirements; y violation which raises questions about the validity of an earlier certification; and	
Guidance		
OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three (3) year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems.		
Applicability: All	References: ARS: CA-6; FISCAM: TSP-5.1.3, TSP-5.2; HSPD 7: F(19); NIST 800-53/53A: CA-6; PISP: 4.4.6	Related Controls: CA-1, CA-2, CA-4, CA-7
ASSESSMENT PROCEDURE: CA-6.1		
Determine if: (i) the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization in accordance with organization-defined frequency, at least every three (3) years; (ii) a senior organizational official signs and approves the security accreditation; (iii) the security accreditation process employed by the organization is consistent with NIST SP 800-37; and (iv) the organization updates the authorization when there is a significant change to the information system. Assessment Methods And Objects Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST SP 800-37; security accreditation package (including information system security plan; security		
	s; authorization statement); other relevant documents or records.	
Interview: Organizational personnel with securit CA-6(0) – Enhancement (Low)		
Control		
	a maximum period of three (3) years, after which the information system must be re-accredited.	
Applicability: All	References: ARS: CA-6(0); NIST 800-53/53A: CA-6; PISP: 4.4.6	Related Controls:
ASSESSMENT PROCEDURE: CA-6(0).1		
Assessment Methods And Objects Examine: Certification and accreditation policy;	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amp procedures addressing security accreditation; NIST SP 800-37; security accreditation package (incluc s; authorization statement); other relevant documents or records.	
CA-7 – Continuous Monitoring (Low)		
Control		
Security controls in CMS information systems sh	all be monitored on an on-going basis. Selection criteria for control monitoring shall be established a	nd a subset of the security controls employed
Pev 0	Page 30 of 127	BPSSM Appendix A Attachment

within information systems shall be selected for continuous monitoring purposes.

Guidance

Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least annually. All other controls are assessed at least annually. All other controls are assessed at least answer requirement (see CA-2).

This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST SP 800-37 provides guidance on the assessment of security controls.

5		
Applicability: All	References: ARS: CA-7; HSPD 7: F(19); NIST 800-53/53A: CA-7; PISP: 4.4.7	Related Controls: CA-2, CA-4, CA-5, CA-
		6, CM-4, SI-2

ASSESSMENT PROCEDURE: CA-7.1

Assessment Objective

Determine if:

(i) the organization monitors the security controls in the information system on an ongoing basis; and

(ii) the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records. **Interview:** Organizational personnel with continuous monitoring responsibilities.(Optional)

ASSESSMENT PROCEDURE: CA-7.2

Assessment Objective

Determine if:

(i) the organization conducts security impact analyses on changes to the information system;

(ii) the organization documents and reports changes to or deficiencies in the security controls employed in the information system; and

(iii) the organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

Interview: Organizational personnel with continuous monitoring responsibilities.(Optional)

CA-7(1) – Enhancement (Low)

Control

The use of independent certification agents or teams is not required but, if used by the organization to monitor the security controls in the information system on an on-going basis, this can be used to satisfy ST&E requirements.

Guidance

The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle.

Applicability: All	References: ARS: CA-7	(1); NIST 800-53/53A: CA-7(1)	Related Controls: AC-9, CA-2
ASSESSMENT PROCEDURE: CA-7(1).1			

Assessment Objective

Determine if the organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.(Optional) **Interview:** Organizational personnel with continuous monitoring responsibilities.(Optional)

CA-7(CMS-1) – Enhancement (Low)

Control

Continuous monitoring activities include:

(a) Configuration management;

(b) Control of information system components;

ASSESSMENT PROCEDURE: CA-7(CMS-1).1

(c) Security impact analyses of changes to the system;

(d) On-going assessment of security controls; and

(e) Status reporting.

Applicability: All

References: ARS: CA-7(CMS-1)

Related Controls:

Assessment Objective

Determine if:

(i) the organization monitors the security controls in the information system on an ongoing basis; and

(ii) the organization employs a security control monitoring process consistent with NIST SP 800-37 and 800-53A.

Assessment Methods And Objects

Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST SP 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records to determine continuous monitoring activities include:

(a) Configuration management;

(b) Control of information system components;

(c) Security impact analyses of changes to the system;

(d) On-going assessment of security controls; and

(e) Status reporting.

Interview: Organizational personnel with continuous monitoring responsibilities to determine continuous monitoring activities include:

(a) Configuration management;

(b) Control of information system components;

(c) Security impact analyses of changes to the system;

(d) On-going assessment of security controls; and

(e) Status reporting.

Configuration Management (CM) – Operational

CM-1 – Configuration Management Policy and Procedures (Low)

Control

A CM process that includes the approval, testing, implementation, and documentation of changes shall be developed, documented, and implemented effectively to track and control the hardware, software, and firmware components that comprise the CMS information system. The CM process shall be consistent with the organization's information technology architecture plans. Formally documented CM roles, responsibilities, procedures, and documentation shall be in place.

Guidance

The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

J		
Applicability: All	References: ARS: CM-1; FISCAM: TCC-2.1.9, TCC-3.2.1, TCC-3.2.2, TCC-3.3.1, TSS-3.1.1, TSS-	Related Controls:
	3.1.2, TSS-3.1.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-1; PISP: 4.5.1	

ASSESSMENT PROCEDURE: CM-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents configuration management policy and procedures;

(ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization;

- (iii) responsible parties within the organization periodically review configuration management policy and procedures; and
- (iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.

Interview: Organizational personnel with configuration management and control responsibilities.(Optional)

ASSESSMENT PROCEDURE: CM-1.2

Assessment Objective

Determine if:

(i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.

Interview: Organizational personnel with configuration management and control responsibilities.(Optional)

CM-2 – Baseline Configuration (Low)

Control

A baseline, operational configuration of the hardware, software, and firmware that comprise the CMS information system shall be developed and documented. Procedures shall be developed, documented, and implemented effectively to maintain the baseline configuration. The configuration of the information system shall be consistent with the Federal Enterprise Architecture and the organization's information system architecture.

Guidance

This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture.

Applicability: All	References: ARS: CM-2; HIPAA: 164.310(b); NIST 800-53/53A: CM-2; PISP: 4.5.2	Related Controls: CM-6, CM-8
ASSESSMENT PROCEDURE: CM-2.1		
Assassment Objective		

Assessment Objective

Determine if:

(i) the organization develops, documents, and maintains a baseline configuration of the information system;

() 3	shows relationships among information system components and is consistent with the Federal En	
()	n provides the organization with a well-defined and documented specification to which the informati	ion system is built; and
., .	nts deviations from the baseline configuration, in support of mission needs/objectives.	
Assessment Methods And O	nagement policy; procedures addressing the baseline configuration of the information system; Fede	aral Enterprise Architecture documentation: information system design
	system architecture and configuration documentation; other relevant documents or records.	ara Enterprise Arcintecture documentation, information system design
CM-2(CMS-1) – Enhancemen		
Control		
	date the baseline configuration and any other system-related operations or security documentation	at least once every year, and while planning major system changes /
upgrades.		rational oneo every year, and while planning major system changes /
Applicability: All	References: ARS: CM-2(CMS-1); FISCAM: TSS-3.2.6	Related Controls:
ASSESSMENT PROCEDURE	E: CM-2(CMS-1).1	
Assessment Objective		
	develops, documents, and maintains a baseline configuration of the information system.	
Assessment Methods And O	Dbjects	
	nagement policy; procedures addressing the baseline configuration of the information system; Fede	
	system architecture and configuration documentation; other relevant documents or records to deter	
	nentation are reviewed and updated at least once every year, and while planning major system cha	
	ersonnel with configuration management responsibilities to determine the baseline configuration and st once every year, and while planning major system changes / upgrades.	a any other system-related operations or security documentation are
CM-2(CMS-2) – Enhancemen		
Control		
	e information system's operations and security documentation.	
Applicability: All	References: ARS: CM-2(CMS-2); FISCAM: TSD-3.1.2, TSD-3.1.3, TSS-3.2.6	Related Controls:
ASSESSMENT PROCEDURE		
Assessment Objective		
-	updates the baseline configuration of the information system as an integral part of information sys	tem component installations.
Assessment Methods And O		
	nagement policy; procedures addressing the baseline configuration of the information system; Fede	eral Enterprise Architecture documentation; information system design
documentation; information s	system architecture and configuration documentation; other relevant documents or records to deter	
security documentation is ma		
	ersonnel with configuration management responsibilities to determine an updated list of the information	tion system's operations and security documentation is maintained.
CM-3 – Configuration Cha	ange Control (Low)	
Control		
	shall be in place and supporting procedures shall be developed, documented, and implemented e	
	to document requests with related approvals. Change requests shall be approved by the Business ig, but not limited to, the system maintainer and information system support staff.	Owner, or his/her designated representative, and other appropriate
organization officials including		
Test plans shall be developed	d and approved for all levels of testing that define responsibilities for each party (e.g., users, syster	m analysts, programmers, auditors, quality assurance, library control)
and shall include appropriate	e consideration of security. Test results shall be documented and appropriate responsive actions sl	hall be taken based on the results.
		ith an animate the share on alterative first. For any state in the state
Emergency changes for the C	CMS information system shall be documented and approved by appropriate organization officials, e ented appropriately and approved, and responsible personnel shall be notified for security analysis	either prior to the change or after the fact. Emergency changes to the
Guidance		
	onfiguration changes to the information system using an organizationally approved process (e.g., a	a chartered Configuration Control Board). Configuration change control
	osal, justification, implementation, test/evaluation, review, and disposition of changes to the information	
change control includes chan	nges to the configuration settings for information technology products (e.g., operating systems, fire	walls, routers). The organization includes emergency changes in the
configuration change control	process, including changes resulting from the remediation of flaws. The approvals to implement a	change to the information system include successful results from the

Applicability: All	References: ARS: CM-3; FISCAM: TCC-1.2.1, TCC-1.2.2, TCC-2.1.1, TCC-2.1.4, TCC-2.1.5, TCC- 2.2.1, TCC-2.2.2, TCC-2.3.1, TCC-3.2.1, TCC-3.2.2, TSS-3.1.3, TSS-3.1.4, TSS-3.1.5; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-3; PISP: 4.5.3	Related Controls: CM-4, CM-6, SI-2
ASSESSMENT PROCEDURE: CM-3	.1	
Assessment Objective		
Determine if:		
(i) the organization authorizes, docur	nents, and controls changes to the information system;	
	rration changes to the information system using an organizationally approved process;	
()	ncy changes in the configuration change control process, including changes resulting from the remediation of flaws	; and
	associated with configuration changes to the information system.	
Assessment Methods And Objects		
5 5	it policy; procedures addressing information system configuration change control; information system architecture a	and configuration documentation; change
	udit records; other relevant documents or records.(Optional)	
CM-3(FIS-1) – Enhancement (Low)		
Control		
	security administrators periodically review production program changes to determine whether access controls and	
Applicability: All	References: FISCAM: TCC-2.1.11	Related Controls:
ASSESSMENT PROCEDURE: CM-3	(FIS-1).1	
Assessment Objective		
Determine if the organization reviews	production program changes for access and change control compliance.	
Assessment Methods And Objects		
Examine: Documentation of manage	ement or security administrator reviews.	
Examine: Pertinent policies and pro		
Interview: Information system mana	gement or security administrators.	
CM-3(FIS-2) – Enhancement (Low)		
Control		
Migration of tested and approved sys	tem software to production use is performed by an independent library control group.	
Applicability: All	References: FISCAM: TSS-3.2.2	Related Controls:
ASSESSMENT PROCEDURE: CM-3	(FIS-2).1	-
Assessment Objective	· · ·	
•	endent library control group migrates tested and approved software into production.	
Assessment Methods And Objects		
Examine: Pertinent policies and proc		
	for some system software migrations.	
	ogrammers, and library control personnel, and determine who migrates approved system software to production lib	raries.
CM-3(FIS-3) – Enhancement (Low)		
Control		
	eduled to minimize the impact on data processing and advance notice is given to system users.	
Applicability: All	References: FISCAM: TSS-3.2.1	Related Controls:
ASSESSMENT PROCEDURE: CM-3		
Assessment Objective	s advance schedules to system users which minimize system software installation impacts.	
Assessment Methods And Objects		
-		
Examine: Pertinent policies and proc	etermine whether scheduling and advance notification did occur.	
	בובווווים שוובנוובו שנוובעמווויץ מווע מעימווכב ווטנווגמנוטוו עוע טכבעו.	
Rev. 9	Page 44 of 127	BPSSM Appendix A. Attachm

Interview: Management and systems program	ners about scheduling and giving advance notices when system software is installed.	
CM-3(FIS-4) – Enhancement (Low)		
Control		
Outdated versions of system software are remo	ved from production libraries.	
Applicability: All	References: FISCAM: TSS-3.2.3	Related Controls:
ASSESSMENT PROCEDURE: CM-3(FIS-4).1	ł	
Assessment Objective		
Determine if the organization removes outdated	versions of system software from the production libraries.	
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation for the rer	noval of outdated versions from production libraries.	
Interview: Management, systems programmers	s, and library control personnel, and determine whether outdated versions are removed from production li	braries.
CM-5 – Access Restrictions for Change	(Low)	
Control		
Access control change mechanisms shall be in	place and supporting procedures shall be developed, documented, and implemented effectively to appro red with changes to the information system. Records reflecting all such changes shall be generated, revi	
Guidance		
Planned or unplanned changes to the hardware	, software, and/or firmware components of the information system can have significant effects on the over ss to information system components for purposes of initiating changes, including upgrades, and modific	erall security of the system. Accordingly, only ations.
Applicability: All	References: ARS: CM-5; FISCAM: TCC-3.2.3, TCC-3.3.1, TSS-1.2.1, TSS-1.2.2, TSS-3.1.4, TSS- 3.2.4; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-5; PISP: 4.5.5	Related Controls:
ASSESSMENT PROCEDURE: CM-5.1		
Assessment Objective		
Determine if:		
	nd authorized personnel permitted to access the information system for the express purpose of initiating	changes.
() 0	privileges and enforces physical and logical access restrictions associated with changes to the information	0
	ews records reflecting all such changes to the information system.	
Assessment Methods And Objects		
	ocedures addressing access restrictions for changes to the information system; information system archi	tecture and configuration documentation:
	it records; other relevant documents or records.(Optional)	······
	estrictions for changes to the information system. (Optional)	
CM-6 – Configuration Settings (Low)		
Control		
	nd implemented effectively to configure and benchmark information technology products in accordance w	vith good security practice settings Mandator
configuration settings for information technology	<i>i</i> products employed within the information system shall be established. The security settings of information	ion technology products shall be configured to
	ation system operational requirements, documented, and enforced in all components of the information s	
Guidance		2
	meters of the information technology products that compose the information system. Organizations moni	tor and control changes to the configuration
	es and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements f	
	onfiguration settings for information technology products employed in organizational information systems	
Applicability: All	References: ARS: CM-6; IRS-1075: 5.6.2.3#1; NIST 800-53/53A: CM-6; PISP: 4.5.6	Related Controls: CM-2, CM-3, CM-8, SI-4
ASSESSMENT PROCEDURE: CM-6.1		1
Assessment Objective		
Determine if:		
(i) the organization establishes mandatory confi	guration settings for information technology products employed within the information system;	
(ii) the organization configures the security settle	ngs of information technology products to the most restrictive mode consistent with operational requirement	
	D 45 6127	

(iii) the organization documents the configuration	n settings: and	
	settings in all components of the information system.	
Assessment Methods And Objects		
	rocedures addressing configuration settings for the information system; information system configuration	settings and associated documentation; NIST
SP 800-70; other relevant documents or record		
Test: Information system configuration settings	.(Optional)	
CM-6(CMS-1) – Enhancement (Low)		
Control		
Configure the information system to provide on application functionality.	y essential capabilities and services by disabling all system services, ports, and network protocols that a	are not explicitly required for system and
Applicability: All	References: ARS: CM-6(CMS-1); IRS-1075: 5.6.2.3#1	Related Controls:
ASSESSMENT PROCEDURE: CM-6(CMS-1)		
Assessment Objective		
Determine if:		
	guration settings for information technology products employed within the information system;	
	ngs of information technology products to the most restrictive mode consistent with operational requiren	nents; and
(iii) the organization documents the configuration	n settings.	
Assessment Methods And Objects		
	rocedures addressing configuration settings for the information system; information system configuration	
	s to determine the information system is configured to provide only essential capabilities and services by	/ disabling all system services, ports, and
network protocols that are not explicitly required		
	uration management responsibilities to determine the information system is configured to provide only e	essential capabilities and services by disabling
· · · · · · · · · · · · · · · · · · ·	Is that are not explicitly required for system and application functionality.	
CM-8 – Information System Componen	t Inventory (Low)	
Control		
	nd implemented effectively to document and maintain a current inventory of the information system's co	
	m components shall include manufacturer, model / type, serial number, version number, location (i.e., pl	nysical location and logical position within the
information system architecture), and ownershi	0.	
Guidance		
	vel of granularity for the information system components included in the inventory that are subject to ma	
	ts includes any information determined to be necessary by the organization to achieve effective property ation, system/component owner). The component inventory is consistent with the accreditation boundar	
Applicability: All	References: ARS: CM-8; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); NIST 800-53/53A: CM-8; PISP:	Related Controls: CM-2, CM-6
	4.5.8	
ASSESSMENT PROCEDURE: CM-8.1	·	
Assessment Objective		
Determine if:		
(i) the organization develops, documents, and r	naintains a current inventory of the components of the information system; and	
(ii) the inventory of information system compon	ents includes any information determined to be necessary by the organization to achieve effective prope	rty accountability.
Assessment Methods And Objects		

Contingency Planning (CP) – Operational

CP-1 – Contingency	Planning Policy	y and Procedures ((Low)

Control

All major CMS information systems shall be covered by a CP that complies with OMB Circular A-130 policy and is consistent with the intent of NIST SP 800-34. Documented procedures shall be developed to facilitate the implementation of the contingency planning policy and associated contingency planning controls. The contingency planning policy and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Contingency planning may result in manual processes in the instance of an actual event, instead of system recovery at an alternate site.

Guidance

The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-34 provides guidance on contingency planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: 1075: 5.6.2.2	,	(7)(i), 164.308(a)(7)(ii)	(B); IRS-	Related Controls:

ASSESSMENT PROCEDURE: CP-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents contingency planning policy and procedures;

(ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review contingency planning policy and procedures; and

(iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: CP-1.2

Assessment Objective

Determine if:

(i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)

CP-2 – Contingency Plan (Low)

Control

All major CMS information systems shall be covered by a CP, relative to the system security level, providing continuity of support in the event of a disruption of service. A CP for the information system shall address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. A CP for the information system shall be consistent with NIST SP 800-34. Designated officials within the organization shall review and approve the CP and distribute copies of the plan to key contingency personnel.

Guidance

Contingency Plans consist of all components listed in the CMS Business Partners system Security Manual, Appendix B; include detailed instructions for restoring operations; and annual training in contingency planning is provided.

Applicability: All	References: ARS: CP-2; FISCAM: TSC-1.1, TSC-1.2, TSC-1.3, TSC-2.1.2, TSC-3.1.1, TSC-3.1.2,	Related Controls:
	TSC-3.1.3, TSC-3.1.4, TSC-3.2.3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i);	
	IRS-1075: 5.6.2.2#1.3; NIST 800-53/53A: CP-2; PISP: 4.6.2	

ASSESSMENT PROCEDURE: CP-2.1

Assessment Objective

(i) the organization develops and documents a contingency plan for the information system;
(ii) the contingency plan is consistent with NIST SP 800-34;
(iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure;
(iv) the contingency plan is reviewed and approved by designated organizational officials; and
(v) the organization disseminates the contingency plan to key contingency personnel.
Assessment Methods And Objects
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; NIST SP 800-34; contingency plan; other relevant documents or records.
ASSESSMENT PROCEDURE: CP-2.2
Assessment Objective
Determine if key contingency personnel and the key operating elements within the organization understand the contingency plan and are ready to implement the plan.
Assessment Methods And Objects
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.(Optional)
CP-3 – Contingency Training (Low)
Control
Operational and support personnel (including managers and users of the information system) shall receive training in contingency operations and understand their contingency roles and
responsibilities with respect to the information system. Refresher training shall be provided to all contingency personnel.
Guidance
Managers, responsible for contingency operations, and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should
be documented and confirmed that appropriate training has been completed.
Applicability: All References: ARS: CP-3; FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-3; PISP: 4.6.3 Related Controls:
ASSESSMENT PROCEDURE: CP-3.1
Assessment Objective
Determine if:
(i) the organization provides contingency training to personnel with significant contingency roles and responsibilities;
(ii) the organization records the type of contingency training received and the date completed;
(iii) the organization defines frequency of refresher contingency training; and
(iv) the organization provides initial training and refresher training in accordance with organization-defined frequency, at least annually.
Assessment Methods And Objects
Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security
plan; other relevant documents or records.(Optional)
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.(Optional)
ASSESSMENT PROCEDURE: CP-3.2
Assessment Objective
Determine if contingency training material addresses the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities.
Assessment Methods And Objects
Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records.(Optional)
CP-3(0) – Enhancement (Low)
Control
Provide training every 365 days in contingency roles and responsibilities.
Applicability: All References: ARS: CP-3(0); FISCAM: TSC-2.3.1; HSPD 7: G(22)(i); PISP: 4.6.3 Related Controls:
ASSESSMENT PROCEDURE: CP-3(0).1
Assessment Objective
Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.
Assessment Methods and Unjects
Assessment Methods And Objects Examine: Contingency planning policy: contingency plan: procedures addressing contingency training: contingency training curriculum: contingency training material: information system security plan
Assessment Methods And Objects Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan Rev. 9 Page 48 of 127 BPSSM Appendix A, Attachment 3

	contingency training); other relevant documents or records. gency planning, plan implementation, and training responsibilities.	
CP-4 – Contingency Plan Testing and Ex		
	ery 365 days using defined tests and exercises, such as the tabletop test in accordance with current CMS Test / exercise results shall be documented and reviewed by appropriate organization officials. Reasor ailures and deficiencies.	
rigor of contingency plan testing and/or exercise effects on organizational operations and assets	ercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, func s increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or ex (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance s for information technology plans and capabilities.	ercises also include a determination of the
Applicability: All	References: ARS: CP-4; FISCAM: TSC-1.1, TSC-4.1, TSC-4.2.1, TSC-4.2.2; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2; NIST 800-53/53A: CP-4; PISP: 4.6.4	Related Controls:
ASSESSMENT PROCEDURE: CP-4.1		
Assessment Objective Determine if: (i) the organization defines the frequency of contingency plan tests and/or exercises; (ii) the organization defines the set of contingency plan tests and/or exercises; (iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency; (iv) the organization documents the results of contingency plan testing/exercises; and (v) the organization reviews the contingency plan test/exercise results and takes corrective actions. Assessment Methods And Objects Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.		
ASSESSMENT PROCEDURE: CP-4.2		
Assessment Objective Determine if the contingency plan tests/exercises Assessment Methods And Objects Examine: Contingency planning policy; continge test results; other relevant documents or records	ncy plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/o	r exercise documentation; contingency plan
CP-4(0) – Enhancement (Low)		
	using a combination of tabletop exercises and operational tests every 365 days, and updated as needed.	
Applicability: All	References: ARS: CP-4(0); FISCAM: TSC-4.1; HSPD 7: G(22)(i); NIST 800-53/53A: CP-4; PISP: 4.6.4	Related Controls:
ASSESSMENT PROCEDURE: CP-4(0).1		
Assessment Methods And Objects Examine: Contingency planning policy; contingency	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify ency plan, procedures addressing contingency plan testing and exercises; information system security pla list of the organization-defined contingency plan tests and/or exercises); contingency plan testing and/or	an (for the organization-defined frequency of
CP-5 – Contingency Plan Update (Low)		
Control CPs shall be reviewed at least every 365 days a	nd, if necessary, revised to address system / organizational changes and/or any problems encountered c	during plan implementation, execution, or
B 0	Decc. 40 of 127	DDCCM A man dim A Attachment 2

testing.		
Guidance		
	hanges in mission, functions, or business processes supported by the information system. The organization communi plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan	
Applicability: All	References: ARS: CP-5; FISCAM: TSC-1.1, TSC-3.1.5; HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	Related Controls:
ASSESSMENT PROCEDURE: CP	P-5.1	
(ii) the organization updates the co	quency of contingency plan reviews and updates; ontingency plan in accordance with organization-defined frequency, at least annually; and e system/organizational changes identified by the organization or any problems encountered by the organization durir	g plan implementation, execution, and testing
Assessment Methods And Object	cts	
• • • • • •	policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security p	lan; other relevant documents or records.
ASSESSMENT PROCEDURE: CP	2-5.2	
Assessment Methods And Object Examine: Contingency planning p	municates necessary changes to the contingency plan to other organizational elements with related plans. cts policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or nel with contingency plan update responsibilities; organizational personnel with mission-related and operational respo	
CP-5(0) – Enhancement (Low)		
Control Review the CP at least every 365 other conditions that may impact the Applicability: All	days and update, as necessary, to address: system, organizational, or facility changes; problems encountered during <u>he system CP.</u> References: ARS: CP-5(0); HSPD 7: G(22)(i); NIST 800-53/53A: CP-5; PISP: 4.6.5	plan implementation, execution, or testing; or Related Controls:
ASSESSMENT PROCEDURE: CP		
Assessment Objective		
-	ts the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this ampl	ifying enhancement to the baseline control.
Assessment Methods And Object	cts	
contingency plan reviews and upd	policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security p lates); other relevant documents or records.	
8 <i>J</i> I 81	policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or	
	nel with contingency plan review and update responsibilities; organizational personnel with mission-related and opera	tional responsibilities.(Optional)
CP-9 – Information System Ba	ackup (Low)	
(including system state information	lace and supporting procedures shall be developed, documented, and implemented effectively to enable the backing- n) contained in the CMS information system. The frequency of information system backups and the transfer rate of back with the CMS recovery time objectives and recovery point objectives.	
time. Backup copies of CMS data	icient backup storage capability. Checkpoint capabilities shall be part of any backup operation that updates files and a shall be created on a regular basis, and appropriate safeguards shall be implemented to protect the technical and phe kup copies of all other forms of data, including paper records, shall be created based upon an assessment of the leve	nysical security of backup media at the storage
Guidance		
and recovery point objectives. Wh	em backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent wit ile integrity and availability are the primary concerns for system backup information, protecting backup information fro ope of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk	m unauthorized disclosure is also an importar
Pay 0	Bage 50 of 127	

information. Checkpoint and restart capabilities transit is beyond the scope of this control.	are part of any operation that updates files and consumes large amounts of computer time. The protection	n of system backup information while in
Applicability: All	References: ARS: CP-9; FISCAM: TSC-2.1.1, TSC-2.1.3; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	Related Controls: MA-CMS-1, MA-CMS-2, MP-4, MP-5
ASSESSMENT PROCEDURE: CP-9.1		
Assessment Objective		
Determine if:		
(i) the organization defines the frequency of info		
(ii) the organization defines the user-level and s	ystem-level information (including system state information) that is required to be backed up; and	
(iii) the organization identifies the location(s) for	storing backup information.	
Assessment Methods And Objects		
Examine: Contingency planning policy; conting or records.	ency plan; procedures addressing information system backup; information system security plan; backup	storage location(s); other relevant documents
ASSESSMENT PROCEDURE: CP-9.2		
Assessment Objective		
Determine if:		
	evel and system-level information (including system state information) in accordance with the organizatio	n-defined frequency;
	n designated locations in accordance with information system backup procedures; and	
(iii) the organization protects backup information	n at the designated storage locations.	
Assessment Methods And Objects		
Examine: Contingency planning policy; conting	ency plan; procedures addressing information system backup; information system security plan; backup	storage location(s); other relevant documents
or records.		
CP-9(0) – Enhancement (Low)		
Control		
· · · · · · · · · · · · · · · · · · ·	information (including system state information) every month.	1
Applicability: All	References: ARS: CP-9(0); HIPAA: 164.308(a)(7)(ii)(A); IRS-1075: 5.6.2.2#1.6; NIST 800-53/53A: CP-9; PISP: 4.6.9	Related Controls:
ASSESSMENT PROCEDURE: CP-9(0).1		
Assessment Objective		
Determine if the organization meets the require	ments as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	ying enhancement to the baseline control.
Assessment Methods And Objects		
•	ency plan; procedures addressing information system backup; information system security plan (for organer relevant documents or records.	nization-defined frequency for information
CP-10 – Information System Recovery a		
Control		
Information system recovery and reconstitution	mechanisms with supporting procedures shall be developed, documented, and implemented effectively to state after a disruption or failure. Recovery of CMS information systems after a failure or other continger	o allow the CMS information system to be ncy shall be done in a trusted, secure, and
Guidance		
are reinstalled, security-related configuration se	to a known secure state means that all system parameters (either default or organization-established) are ttings are reestablished, system documentation and operating procedures are available, application and s recent, known secure backups is loaded, and the system is fully tested.	e set to secure values, security-critical patches system software is reinstalled and configured
Applicability: All	References: ARS: CP-10; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST 800-53/53A: CP-10; PISP: 4.6.10	Related Controls:
ASSESSMENT PROCEDURE: CP-10.1		
Assessment Objective		
-	ns for capturing the information system's operational state including appropriate system parameters, pate	hes, configuration settings, and

application/system software prior to system	disruption or failure.			
Assessment Methods And Objects				
Examine: Contingency planning policy; con	tingency plan; procedures addressing information system recovery and reconstitution; information	on system configuration settings and associated		
documentation; information system design of	locumentation; other relevant documents or records.			
ASSESSMENT PROCEDURE: CP-10.2				
Assessment Objective				
Determine if the organization makes availab	le and applies mechanisms and procedures for recovery and reconstitution of the information sy	ystem to known secure state after disruption or failure.		
Assessment Methods And Objects				
	Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.			
Test: Automated mechanisms implementing	Test: Automated mechanisms implementing information system recovery and reconstitution operations. (Optional)			
CP-10(0) – Enhancement (Low)				
Control				
Secure information system recovery and rec	onstitution includes, but not limited to:			
(a) Reset all system parameters (either defa	ult or organization-established),			
(b) Reinstall patches,				
(c) Reestablish configuration settings,				
(d) Reinstall application and system softwar	e, and			
(e) Fully test the system.				
Applicability: All	References: ARS: CP-10(0); NIST 800-53/53A: CP-10; PISP: 4.6.10	Related Controls:		
ASSESSMENT PROCEDURE: CP-10(0).1				
Assessment Objective				
Determine if the organization meets the requ	uirements as specified in the baseline control and the specific CMS requirements as prescribed	in this amplifying enhancement to the baseline control.		
Assessment Methods And Objects				

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

1

Identification and Authentication (IA) – Technical

IA-1 – Identification and Authentication Policy and Procedures (Low)

Control

Automated IA mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and sensitivity of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. The IA procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, FIPS 201, NIST SP 800-63, NIST SP 800-73, and NIST SP 800-76.

Guidance

The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and SP 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-63 provides guidance on remote electronic authentication.

Applicability: All	References: ARS: IA-1; IRS-1075: 5.6.3.1#1.1; NIST 800-53/53A: IA-1; PISP: 4.7.1	Related Controls:
ASSESSMENT PROCEDURE: IA-1.1		

Assessment Objective

Determine if:

(i) the organization develops and documents identification and authentication policy and procedures;

(ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review identification and authentication policy and procedures; and

(iv) the organization updates identification and authentication policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.

Interview: Organizational personnel with identification and authentication responsibilities.(Optional)

ASSESSMENT PROCEDURE: IA-1.2

Assessment Objective

Determine if:

(i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.

Interview: Organizational personnel with identification and authentication responsibilities.(Optional)

IA-2 – User Identification and Authentication (Low)

Control

Automated IA mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enable unique IA of individual users (or processes acting in behalf of users) of CMS information systems. Authentication of user identities shall be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein.

Guidance

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in SP 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST SP 800-63 level 1 compliant. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide information security for the organization.

privacy-related information. The e-authentication such accesses with regard to the IA-2 control ar	ation E-Government initiative, authentication of public users accessing federal information systems may n risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NI nd its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancements with the need to protect organizational operations, organizational assets, and individuals.	ST SP 800-63 compliance requirements for
Applicability: All	References: ARS: IA-2; FISCAM: TAC-3.2.A.4, TAN-2.1.4; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 5.6.3.1#1.2, 5.6.3.3#2.3; NIST 800-53/53A: IA-2; PISP: 4.7.2	Related Controls: AC-14, AC-17, MA-4
ASSESSMENT PROCEDURE: IA-2.1		
	d authenticates users (or processes acting on behalf of users); and acting on behalf of users) are consistent NIST SP 800-63 and e-authentication risk assessment results.	
assessment results; information system configu Test: Automated mechanisms implementing ide	y; NIST SP 800-63; procedures addressing user identification and authentication; information system de ration settings and associated documentation; information system audit records; other relevant documen entification and authentication capability for the information system.(Optional)	
IA-2(CMS-1) – Enhancement (Low)		
Control		
Require the use of unique user identifiers and s		
Applicability: All	References: ARS: IA-2(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4, TAN-2.1.4, TAN-2.1.7; IRS-1075: 5.6.3.1#1.2	Related Controls:
ASSESSMENT PROCEDURE: IA-2(CMS-1).1		
configuration settings and associated document network authenticators is required.	ry; NIST SP 800-63; procedures addressing user identification and authentication; information system de ation; information system audit records; other relevant documents or records to determine the use of uni ication and authentication responsibilities to determine the use of unique user identifiers and system and	que user identifiers and system and/or
Control		
All passwords shall be encrypted in transit and a	at rest.	
Applicability: All	References: ARS: IA-2(CMS-2); FISCAM: TAC-3.2.A.1, TAC-3.2.A.7; IRS-1075: 5.6.3.1#1.2	Related Controls:
ASSESSMENT PROCEDURE: IA-2(CMS-2).1		
Assessment Methods And Objects Examine: Identification and authentication polic configuration settings and associated document	processes acting on behalf of users) are consistent NIST SP 800-63. by; NIST SP 800-63; procedures addressing user identification and authentication; information system de ation; information system audit records; other relevant documents or records to determine all passwords	
	ication and authentication responsibilities to determine to determine all passwords are required to be end	crypted in transit and at rest.
IA-2(CMS-3) – Enhancement (Low)		
Control		
· · · · ·	r any transaction that has information security implications.	Deleted Operate
Applicability: All	References: ARS: IA-2(CMS-3)	Related Controls:
ASSESSMENT PROCEDURE: IA-2(CMS-3).1 Assessment Objective Determine if authentication levels for users (or p	processes acting on behalf of users) are consistent NIST SP 800-63.	
Rev. 9	Page 54 of 127	BPSSM Appendix A, Attachment

Assessment Methods And Objects

Examine: Identification and authentication policy; NIST SP 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine help desk support requires user identification for any transaction that has information security implications.

Interview: Organizational personnel with identification and authentication responsibilities to determine to determine help desk support requires user identification for any transaction that has information security implications.

IA-3 – Device Identification and Authentication (Low)

Control

Automated mechanisms shall be used to enable IA of the CMS information system being used and to which a connection is being made before establishing a connection.

Guidance

The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802. 1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Applicability: All	References: ARS: IA-3; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-3; PISP: 4.7.3	Related Controls:
ASSESSMENT PROCEDURE: 1A-3.1		

ASSESSMENT PROCEDURE: IA-3.1

Assessment Objective

Determine if:

(i) the organization defines specific devices requiring identification and authentication before establishing connections to the information system; and

(ii) the information system identifies and authenticates specific devices identified by the organization before establishing connections.

Assessment Methods And Objects

Examine: Identification and authentication policy: procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation: other relevant documents or records.(Optional)

Test: Automated mechanisms implementing device identification and authentication.(Optional)

IA-3(0) – Enhancement (Low)

Control

Implement an information system that uses either a shared secret or digital certificate to identify and authenticate specific devices before establishing a connection.

Applicability: All	References: ARS: IA-3(0); IRS-1075: 5.6.3.1#1.2; PISP: 4.7.3	Related Controls:

ASSESSMENT PROCEDURE: IA-3(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Identification and authentication policy: information system design documentation; procedures addressing device identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.

IA-4 – Identifier Management (Low)

Control

Procedures shall be developed, documented, and implemented effectively to manage user identifiers. The procedures shall address processes and controls for:

4.7.4.1. Identifying each user uniquely;

4.7.4.2. Verifying the identity of each user:

4.7.4.3. Receiving authorization to issue a user identifier from an appropriate organization official;

4.7.4.4. Ensuring that the user identifier is issued to the intended party:

4.7.4.5. Disabling user identifier after a specific period of inactivity; and

4.7.4.6. Archiving user identifiers.

Reviews and validation of system users' accounts shall be conducted to ensure the continued need for access to a system. Identifier management shall not be applicable to shared information system accounts (i.e., guest and anonymous).

Guidance

Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity

verification (PIV) credential for use in the unique	e identification and authentication of federal employees and contractors.		
Applicability: All	References: ARS: IA-4; FISCAM: TAC-3.2.A.4, TAN-2.1.4; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-4; PISP: 4.7.4	Related Controls:	
ASSESSMENT PROCEDURE: IA-4.1			
Assessment Objective			
Determine if:			
(i) the organization manages user identifiers by			
(ii) the organization manages user identifiers by			
	y receiving authorization to issue a user identifier from an appropriate organization official;		
(iv) the organization manages user identifiers b			
	nactivity after which a user identifier is to be disabled; y disabling the identifier after the organization-defined time period of inactivity; and		
(vii) the organization manages user identifiers b			
Assessment Methods And Objects			
-	cy; procedures addressing identifier management; information system security plan; information system d	lesign documentation: information system	
configuration settings and associated documen	tation; list of information system accounts; other relevant documents or records.		
	mation system and for organizational facilities.(Optional)		
ASSESSMENT PROCEDURE: IA-4.2			
Assessment Objective			
Determine if the organization uses a Personal I	dentity Verification (PIV) card token to uniquely identify and authenticate federal employees and contract	ors in accordance with FIPS 201 and NIST SP	
800-73, 800-76, and 800-78.			
Assessment Methods And Objects			
	cy; procedures addressing identifier management; information system design documentation; FIPS 201; I	NIST SP 800-73, 800-76, 800-78; information	
	ocumentation; list of information system accounts; other relevant documents or records.		
	mation system and for organizational facilities.(Optional)		
IA-4(0) – Enhancement (Low)			
Control			
	ity and delete disabled accounts during annual re-certification process.	1	
Applicability: All	References: ARS: IA-4(0); FISCAM: TAC-3.2.C.4; IRS-1075: 5.6.3.1#2, 5.6.3.2#2.1; NIST 800- 53/53A: IA-4; PISP: 4.7.4	Related Controls: AC-2(3)	
ASSESSMENT PROCEDURE: IA-4(0).1			
Assessment Objective			
	ments as specified in the baseline control and the specific CMS requirements as prescribed in this amplif	fying enhancement to the baseline control.	
Assessment Methods And Objects			
	Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user		
, · · · · · · · · · · · · · · · · · · ·	identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant		
documents or records. Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST SP 800-73, 800-76, 800-78; information			
	cy; procedures addressing identifier management; information system design documentation; FIPS 201; I ocumentation; list of information system accounts; other relevant documents or records.	NIST SP 800-73, 800-76, 800-78; Information	
IA-4(CMS-1) – Enhancement (Low)			
Control			
	ate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for syst	stem administration activities	
Applicability: All	References: ARS: IA-4(CMS-1); FISCAM: TAC-3.2.A.1, TAC-3.2.A.4; IRS-1075: 5.6.3.1#2	Related Controls: AC-2(CMS-2)	
ASSESSMENT PROCEDURE: IA-4(CMS-1).1			
Assessment Objective			
-	patifiers by uniquely identifying each user		
Determine if the organization manages user ide			

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan (for organization-defined time period of inactivity after which user identifier is to be disabled); information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.

Interview: Organizational personnel with identification and authentication responsibilities to determine system administrators maintain separate user accounts; one exclusively for standard user functions (e.g., Internet, email, etc.), and one for system administration activities.

IA-4(CMS-2) – Enhancement (Low)

Control

For non-CMS entities to issue user identifiers, receive prior written approval from the CIO or his/her designated representative.

Applicability: All References: ARS: IA-4(CMS-2)

ASSESSMENT PROCEDURE: IA-4(CMS-2).1

Assessment Objective

Determine if responsible parties within the organization periodically review identification and authentication policy and procedures.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers.

Interview: Organizational personnel with identification and authentication management responsibilities to determine non-CMS entities receive prior written approval from the CIO or his/her designated representative before issuing user identifiers.

IA-4(FIS-1) – Enhancement (Low)

Control

Personnel files are matched with actual system users to remove terminated or transferred employees from the system.

 Applicability: All
 References: FISCAM: TAC-3.2.A.6
 Related Controls:

ASSESSMENT PROCEDURE: IA-4(FIS-1).1

Assessment Objective

Determine if the organizational personnel files are matched with actual system users to remove terminated or transferred employees from the system.

Assessment Methods And Objects

Examine: Documentation of such comparisons.

Examine: Pertinent policies and procedures.

Interview: Security managers.

IA-5 – Authenticator Management (Low)

Control

Procedures shall be developed, documented, and implemented effectively to manage user authenticators. The procedures shall address processes and controls for: initial authenticator content; distribution for new, lost, compromised, or damaged authenticators; revocation of authenticators; changing default authenticators; and changing / refreshing authenticators at specified intervals. Users shall not loan or share authenticators with other users. Lost or compromised authenticators shall be reported immediately to appropriate authority.

Selection of passwords or other authentication devices (e.g., tokens, biometrics) shall be appropriate, based on the CMS System Security Level of the information system. Automated mechanisms shall be in place for password-based authentication, to ensure that the information system:

4.7.5.1. Protects passwords from unauthorized disclosure and modification when stored and transmitted;

4.7.5.2. Prohibits passwords from being displayed when entered;

4.7.5.3. Enforces automatic expiration of passwords;

4.7.5.4. Prohibits password reuse for a specified number of generations; and

4.7.5.5. Enforces periodic password changes.

Guidance

Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i)

Related Controls:

validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and SP 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication.

identification and authentication of federal emplo	byees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication.	
Applicability: All	References: ARS: IA-5; FISCAM: TAC-3.2.A.1, TAC-3.2.A.3; IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	Related Controls: AC-11(0), AC-CMS- 1(CMS-2)
ASSESSMENT PROCEDURE: IA-5.1		
Assessment Objective Determine if: (i) the organization manages information system (ii) the organization manages information system for revoking authenticators; (iii) the organization manages information system (iv) the organization manages information system Assessment Methods And Objects Examine: Identification and authentication policy associated documentation; list of information system IA-5(0) – Enhancement (Low) Control	a authenticators by defining initial authenticator content; n authenticators by establishing administrative procedures for initial authenticator distribution, for lost/com n authenticators by changing default authenticators upon information system installation; and n authenticators by changing/refreshing authenticators periodically. y; procedures addressing authenticator management; information system design documentation; informa stem accounts; other relevant documents or records.	npromised, or damaged authenticators, and
 (d) Force users to select a password comprising (e) Automatically force users (including administ (f) Automatically force users to select one (1) un 	,	
Applicability: All	References: ARS: IA-5(0); HIPAA: 164.308(a)(5)(ii)(D); IRS-1075: 5.6.3.1#2; NIST 800-53/53A: IA-5; PISP: 4.7.5	Related Controls:
ASSESSMENT PROCEDURE: IA-5(0).1		
Assessment Methods And Objects Examine: Identification and authentication policy	nents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify y; procedures addressing authenticator management; information system design documentation; informa stem accounts; other relevant documents or records.	
IA-5(FIS-1) – Enhancement (Low)		
Control For devices such as tokens or key cards, users: lost items immediately.	(1) maintain possession of their individual tokens, cards, etc., and (2) understand that they must not loan	or share these with others, and must report
Applicability: All	References: FISCAM: TAC-3.2.A.8	Related Controls:
ASSESSMENT PROCEDURE: IA-5(FIS-1).1		
	of their individual devices such as tokens or key cards, etc.; and st not loan or share their individual tokens, cards, etc., and report lost items immediately.	

Examine: Token or key card acknowledgment	forms.	
Interview: Token and/or key card users.		
IA-5(DIR-1) – Enhancement (Low)		
Control		
For password-based authentication, passwords (a) unique for specific individuals, not groups;	s are:	
(a) unique for specific individuals, not groups, (b) controlled by the assigned user and not sub	iect to disclosure:	
(c) not displayed when entered;		
	changes positions, or when security is breached;	
(e) at least 8 characters in length;		
	r and lower case character, and one special character;	
(g) prohibited from reuse for at least 6 generation		
(h) prohibited from being changed more than or (i) all passwords are encrypted in transit and at	rest. The use of dictionary names or words as passwords is prohibited.	
Applicability: All	References: FISCAM: TAC-3.2.A.1, TAC-3.2.A.2, TAN-2.1.4	Related Controls:
ASSESSMENT PROCEDURE: IA-5(DIR-1).1		Trefated Controls.
Assessment Objective		
-	assword and user identification as one tool for security in-depth.	
Assessment Methods And Objects	assword and user identification as one too for security in-depth.	
	icy and acceptable user training policy for completeness in meeting the CMS password controls.	
	ization's policy for password and user system identification.	
IA-6 – Authenticator Feedback (Low)		
Control		
	nd supporting procedures shall be developed, documented, and implemented effectively to obscure fea	edback to users during the authentication process
to protect the information from possible exploita		addata to doolo during the durionited on proceed
Guidance		
The feedback from the information system does	s not provide information that would allow an unauthorized user to compromise the authentication mec	hanism. Displaying asterisks when a user types
in a password is an example of obscuring feed	pack of authentication information.	
Applicability: All	References: ARS: IA-6; IRS-1075: 5.6.3.1#1.2; NIST 800-53/53A: IA-6; PISP: 4.7.6	Related Controls:
ASSESSMENT PROCEDURE: IA-6.1		
Assessment Objective		
	eedback of authentication information during the authentication process to protect the information from	possible exploitation/use by unauthorized
individuals.		
Assessment Methods And Objects		
	cy; procedures addressing authenticator feedback; information system design documentation; informat	ion system configuration settings and associated
documentation; other relevant documents or re		
Test: Automated mechanisms implementing au		
IA-6(0) – Enhancement (Low)		
Control		
	Asswords during the authentication process (e.g., display asterisks). References: ARS: IA-6(0); FISCAM: TAC-3.2.A.1; NIST 800-53/53A: IA-6; PISP: 4.7.6	Related Controls:
	References: ARS. IA-6(0), FISCAWI. TAC-3.2.A.T, NIST 800-53/53A. IA-6, PISP. 4.7.6	Related Controls.
ASSESSMENT PROCEDURE: IA-6(0).1		
Assessment Objective	mente on appointed in the boarding control and the creatify OMO requirements or present with this set	nlift in a anhan a mant to the baseline sector
-	ments as specified in the baseline control and the specific CMS requirements as prescribed in this am	pinying enhancement to the baseline control.
Assessment Methods And Objects	av propoduros addressing authenticator feedback information system design desum-stations information	ion austam configuration cattings and appaciated
documentation; other relevant documents or re	cy; procedures addressing authenticator feedback; information system design documentation; informat cords.	ion system configuration settings and associated
		·
Rev. 9	Page 59 of 127	BPSSM Appendix A, Attachment 3

IA-7 – Cryptographic Module Authentication (Low)

Control

Authentication to a cryptographic module shall require the CMS information system to employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Guidance

The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Applicability: All	References: ARS: IA-7; NIST 800-53/53A: IA-7; PISP: 4.7.7	Related Controls:
ASSESSMENT PROCEDURE: IA-7.1		

Assessment Objective

Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).

Assessment Methods And Objects

Examine: Identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Automated mechanisms implementing cryptographic module authentication.(Optional)

Incident Response (IR) - Operational

IR-1 – Incident Response Policy and Procedures (Low)

Control

An IR plan shall be developed, disseminated and reviewed / updated periodically to address the implementation of IR controls. IR procedures shall be developed, documented, and implemented effectively to monitor and respond to all IS incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, NIST SP 800-61 and current CMS Procedures.

Guidance

The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

	55/55A. IN-1, FISF. 4.0.1	
	53/53A: IR-1; PISP: 4.8.1	
Applicability: All	References: ARS: IR-1; FISCAM: TSP-3.4; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1; NIST 800-	Related Controls:

ASSESSMENT PROCEDURE: IR-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents incident response policy and procedures;

(ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review incident response policy and procedures; and

(iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.

Interview: Organizational personnel with incident response planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: IR-1.2

Assessment Objective

Determine if:

(i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.

Interview: Organizational personnel with incident response planning and plan implementation responsibilities.(Optional)

IR-4 – Incident Handling (Low)

Control

An incident handling capability, which includes preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents, shall be established and maintained. Evidence of computer crimes, computer misuse, and all other unlawful computer activities shall be properly preserved. Lessons learned from on-going incident handling activities shall be incorporated into the IR procedures.

Guidance

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.

Applicability: All	References: ARS: IR-4; HIPAA 53/53A: IR-4; PISP: 4.8.4	: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1	, 5.6.2.6#2.3; NIST 800-	Related Controls: AU-6, PE-6, SI-2
ASSESSMENT PROCEDURE: IR-4.1				

Assessment Objective

Determine if:

(i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and

	White an electron with NICT CD 000 04	
	vility is consistent with NIST SP 800-61.	
Assessment Methods And Ob		4-
	olicy; procedures addressing incident handling; NIST SP 800-61; other relevant documents or record sonnel with incident handling responsibilities.(Optional)	JS.
	lity for the organization.(Optional)	
IR-4(CMS-1) – Enhancement (I		
	LOW)	
Control	a related to a acquirity incident according to CMS Information Security Incident Handling and Press N	Notification Broaduroa
	n related to a security incident according to CMS Information Security Incident Handling and Breach N References: ARS: IR-4(CMS-1); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	
		Related Controls:
ASSESSMENT PROCEDURE:	IR-4(CMS-1).1	
Assessment Objective		
Determine if:	a an insident handling conchility for acquirity insidents that includes proparation, detection and analysis	in containment aradiantian and recovery and
	s an incident handling capability for security incidents that includes preparation, detection and analysi sility is consistent with NIST SP 800-61.	is, containment, eradication, and recovery, and
Assessment Methods And Ob	•	
	olicy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents	a or records to determine if relevant information related to a security
	ling to the CMS Information Security Incident Handling capability, MST SP 800-61, other relevant documents	s of records to determine in relevant information related to a security
	sonnel with incident response training and operational responsibilities to determine if relevant informa	ation related to a security incident is documented according to the
	dent Handling and Breach Notification Procedures.	
IR-4(CMS-2) – Enhancement (I		
Control		
	chnical means, including secured storage of evidence media and "write" protection of evidence media	Lise sound forensics processes and utilities that support legal
	follow chain of custody for forensic evidence.	
Applicability: All	References: ARS: IR-4(CMS-2); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	Related Controls:
ASSESSMENT PROCEDURE:	IR-4(CMS-2).1	
Assessment Objective		
Determine if:		
() S	s an incident handling capability for security incidents that includes preparation, detection and analysi	is, containment, eradication, and recovery; and
	ility is consistent with NIST SP 800-61.	
Assessment Methods And Ob		
	olicy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents	
<i>,</i> 0	age of evidence media and "write" protection of evidence media; sound forensics processes and utilit	ties are used that support legal requirements. A chain of custody
for forensic evidence is followed	a. sonnel with incident response training and operational responsibilities to determine if evidence is pres	conved through technical means, including accured storage of
	otection of evidence media; sound forensics processes and utilities are used that support legal require	
IR-4(CMS-3) – Enhancement (I		
	LOW	
Control		
	during a security incident. Implement security safeguards to reduce risk and vulnerability exploit expo References: ARS: IR-4(CMS-3); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	
		Related Controls:
ASSESSMENT PROCEDURE:	IR-4(CINS-3).1	
Assessment Objective		
Determine if:	a an incident bondling appohility for a privity incidents that includes proportion, data of a second solution	in containment analization and recovery and
	s an incident handling capability for security incidents that includes preparation, detection and analysi	ils, containment, eradication, and recovery; and
	vility is consistent with NIST SP 800-61.	
Assessment Methods And Ob		o or records to determine if the identification of unit are tilting
	olicy; procedures addressing incident handling capability; NIST SP 800-61; other relevant documents dent and security safeguards are implemented to reduce risk and vulnerability exploit exposure.	s or records to determine it the identification of vulnerabilities

	t response training and operational responsibilities to determine if the identification	n of vulnerabilities exploited during a security incident and security
safeguards are implemented to reduce risk and v IR-6 – Incident Reporting (Low)	vulnerability exploit exposure.	
Control		
	reported to the CMS IT Service Desk (or equivalent organizational function) as so	on as an incident comes to the attention of a user of CMS
	confirmed security incidents by business partners shall also be reported to the CM	
Guidance		
Orders, directives, policies, regulations, standard http://www.us-cert.gov within the specified timefr and vulnerabilities in the information system are reporting.	ontent and timeliness of the reports, and the list of designated reporting authorities ds, and guidance. Organizational officials report cyber security incidents to the Unit ame designated in the US-CERT Concept of Operations for Federal Cyber Securit reported to appropriate organizational officials in a timely manner to prevent secure	ited States Computer Emergency Readiness Team (US-CERT) at ity Incident Handling. In addition to incident information, weaknesses rity incidents. NIST SP 800-61 provides guidance on incident
Applicability: All	References: ARS: IR-6; FISCAM: TAC-4.2; NIST 800-53/53A: IR-6; PISP: 4.8.6	Related Controls:
ASSESSMENT PROCEDURE: IR-6.1		
Assessment Objective		
Determine if:		
(i) the organization promptly reports incident info		
(ii) incident reporting is consistent with NIST SP		
 (iii) the types of incident information reported, the regulations, standards, and guidance; and 	e content and timeliness of the reports, and the list of designated reporting is consi	istent with applicable laws, Executive Orders, directives, policies,
(iv) weaknesses and vulnerabilities in the information	ation system are reported to appropriate organizational officials in a timely manner	r to prevent security incidents.
Assessment Methods And Objects		
Examine: Incident response policy; procedures Interview: Organizational personnel with incider	addressing incident reporting; NIST SP 800-61; incident reporting records and doc at reporting responsibilities.(Optional)	cumentation; other relevant documents or records.
Test: Incident reporting capability for the organiz		
IR-7 – Incident Response Assistance (L		
Control		
	ional function) shall be in place and shall play an appropriate role in the organization shall be developed, documented, and implemented effectively to facilitate the incident shall be developed.	
Guidance		
Possible implementations of incident response s	upport resources in an organization include a help desk or an assistance group an	nd access to forensics services, when required.
Applicability: All	References: ARS: IR-7; NIST 800-53/53A: IR-7; PISP: 4.8.7	Related Controls:
ASSESSMENT PROCEDURE: IR-7.1		
Assessment Objective		
Determine if:		
(i) the organization provides an incident respons	e support resource that offers advice and assistance to users of the information sy	stem for the handling and reporting of security incidents; and
	integral part of the organization's incident response capability.	
Assessment Methods And Objects		
Example a local device and a set of the set		
	addressing incident response assistance; other relevant documents or records. It response assistance and support responsibilities.(Optional)	

Maintenance (MA) - Operational

MA-1 – System Maintenance Policy and Procedures (Low)

Control

System maintenance shall be employed on all CMS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance. Maintenance of software shall include the installation of all relevant patches and fixes required to correct security flaws in existing software and to ensure the continuity of business operations.

Guidance

The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: MA-1; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3; NIST 800-53/53A: MA-1; PISP: 4.9.1	Related Controls:

ASSESSMENT PROCEDURE: MA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents information system maintenance policy and procedures;

(ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review information system maintenance policy and procedures; and

(iv) the organization updates information system maintenance policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

ASSESSMENT PROCEDURE: MA-1.2

Assessment Objective

Determine if:

(i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-1(FIS-1) – Enhancement (Low)

Control

All system software is current, has current and complete documentation, and is still supported by the vendor.

Applicability: All	References: FISCAM: TSS-3.2.5, TSS-3.2.6	Related Controls:
ASSESSMENT PROCEDURE: MA-1(FIS-1).1		

Accessment Objective

Assessment Objective

Determine if the organization uses current system software with complete documentation and is vendor supported.

Assessment Methods And Objects

Examine: Pertinent policies and procedures.

Interview: Management and systems programmers about the currency of system software, and the currency and completeness of software documentation.

Interview: System software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.

MA-2 – Controlled Maintenance (Low)

Control

Comprehensive maintenance procedures shall be developed, documented, and implemented effectively to conduct controlled periodic on-site and off-site maintenance of the CMS information

systems and of the physical plant within which these information systems reside. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Appropriate officials shall approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, all information from associated media shall be removed using CMS-approved procedures. After maintenance is performed on the information system, the security features shall be tested to ensure that they are still functioning properly. **Guidance**All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or removel and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system or information system or system or information system or information system or system or information system or system or system or system or system or information system or system or information system or information system or system or information system o

another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Applicability: All; Optional for SS	References: ARS: MA-2; FISCAM: TSC-2.4.1, TSC-2.4.2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2,	Related Controls:
	5.6.2.4#1.3; NIST 800-53/53A: MA-2; PISP: 4.9.2	

ASSESSMENT PROCEDURE: MA-2.1

Assessment Objective

Determine if the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-2(FIS-1) – Enhancement (Low) Control Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance. Applicability: All References: FISCAM: TSC-2.4.4 **Related Controls:** ASSESSMENT PROCEDURE: MA-2(FIS-1).1 Assessment Objective Determine if the organization accommodates regular and a reasonable amount of unscheduled maintenance in its data processing operations. **Assessment Methods And Objects** Examine: Maintenance documentation. Examine: Pertinent policies and procedures. Interview: Data processing and user management. MA-2(FIS-2) – Enhancement (Low) Control Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users thus allowing for adequate testing. Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted References: FISCAM: TSC-2.4.10, TSC-2.4.11 **Related Controls:** Applicability: All ASSESSMENT PROCEDURE: MA-2(FIS-2).1 **Assessment Objective** Determine if: (i) the organization schedules hardware equipment and related software changes such to minimize user impact and maximize resources for adequate testing; and (ii) the organizational advance notification for hardware equipment changes does not cause unexpected interrupted user services. **Assessment Methods And Objects** Examine: Pertinent policies and procedures.

Examine: Supporting documentation.

Interview: Senior management, data processing management, and user management.

MA-3 – Maintenance Tools (Low) Control The use of system maintenance tools, including diagnostic and test equipment and administration utilities, shall be approved, controlled, and monitored. Approved tools shall be maintained on an ongoing basis. Guidance The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "Is," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control. References: ARS: MA-3: IRS-1075: 5.6.2.4#1.2, 5.6.2.4#1.3: NIST 800-53/53A: MA-3: PISP: 4.9.3 Applicability: All **Related Controls: ASSESSMENT PROCEDURE: MA-3.1 Assessment Objective** Determine if: (i) the organization approves, controls, and monitors the use of information system maintenance tools; and (ii) the organization maintains maintenance tools on an ongoing basis. Assessment Methods And Objects Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records: other relevant documents or records.(Optional) MA-4 – Remote Maintenance (Low) Control Remote maintenance of a CMS information system must be approved by the CIO or his/her designated representative. Remote maintenance procedures shall be developed, documented, and implemented effectively to provide additional controls on remotely executed maintenance and diagnostic activities. The use of remote diagnostic tools shall be described in the SSP for the information system. Maintenance records for all remote maintenance, diagnostic, and service activities shall be maintained and shall be reviewed periodically by appropriate organization officials. All sessions and remote connections shall be terminated after the remote maintenance is completed. If password-based authentication is used during remote maintenance, the passwords shall be changed following each remote maintenance service. Guidance Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications: (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST SP 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm. References: ARS: MA-4: FISCAM: TAC-2.1.3: IRS-1075: 5.6.2.4#1.1. 5.6.2.4#1.2. 5.6.2.4#1.3: NIST Applicability: All Related Controls: IA-2. MP-6 800-53/53A: MA-4: PISP: 4.9.4 **ASSESSMENT PROCEDURE: MA-4.1** Assessment Objective Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed. **Assessment Methods And Objects** Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; information system design documentation; information system configuration settings and associated documentation: maintenance records: other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities.(Optional) MA-4(CMS-1) – Enhancement (Low) Control If remote maintenance is authorized in writing by the CIO or his/her designated representative: Encrypt and decrypt diagnostic communications: utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, terminate all sessions and remote connections. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service. Applicability: All References: ARS: MA-4(CMS-1) **Related Controls:**

ASSESSMENT PROCEDURE: MA-4(CMS-1).1

Assessment Objective

Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine that remote maintenance is authorized in writing by the CIO or his/her designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service.

Interview: Organizational personnel with information system maintenance responsibilities to determine that remote maintenance is authorized in writing by the CIO or his/her designated representative: diagnostic communications are encrypted / decrypted; utilize strong identification and authentication techniques, such as tokens; and when remote maintenance is completed, all sessions and remote connections are terminated. If password-based authentication is used during remote maintenance, the passwords are changed following each remote maintenance service.

MA-5 – Maintenance Personnel (Low)

Control

Maintenance personnel procedures shall be developed, documented, and implemented effectively to control maintenance of CMS information systems. A list of individuals authorized to perform maintenance on the information system shall be maintained.

Guidance

Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Applicability: All	References: ARS: MA-5; NIST 800-53/53A: MA-5; PISP: 4.9.5	Related Controls:
ASSESSMENT PROCEDURE: MA-5.1		
Accomment Objective		

Assessment Objective

Determine if the organization allows only authorized personnel to perform maintenance on the information system.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-5(0) – Enhancement (Low)

Control

Only authorized individuals are allowed to perform maintenance. Ensure maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. Supervise maintenance personnel during the performance of maintenance activities when they do not have the needed access authorizations.

Applicability: All	References: ARS: MA-5(0); HIPA	AA: 164.308(a)(3)(ii)(A); NIST 800-53/53A: MA-5;	PISP: 4.9.5	Related Controls:
ASSESSMENT PROCEDURE: MA-5(0).1				

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records.

Interview: Organizational personnel with information system maintenance responsibilities.(Optional)

MA-CMS-1 – Off-site Physical Repair of Systems (Low)

Control

Controls shall be developed, documented, and implemented effectively to enable off-site physical repair of systems without compromising security functionality or confidentiality.

Guidance

It is good practice to complete a full security review of a system before it is put back into operation when the system has returned from off-site repair. The repaired system should match the approved Change Management baseline.

Storage media control when encrypted may take special considerations.

Applicability: All	References: ARS: MA-CMS-1; PISP: 4.9.7	Related Controls: AC-19(CMS-1), AC-3,

		CP-9, SC-12(CMS-1)	
ASSESSMENT PROCEDURE: MA-CMS-1.1			
Assessment Objective			
	s procedures, documents procedures, and implements off-site repair of s	systems without compromising security functionality or confidentiality.	
Assessment Methods And Objects			
Examine: Information system maintenance pole repair.	y and procedures; other relevant documents or records to determine that	t only authorized personnel are permitted access to the system for off-site	
	ation system maintenance responsibilities to determine that only authoriz	ed personnel are permitted access to systems during off-site repair.	
MA-CMS-1(CMS-0) – Enhancement (Low)			
Control			
	ed personnel only. Storage media must be removed before shipment for ormed, check security features to verify they are functioning properly.	repairs. Unusable storage media must be degaussed or destroyed by	
Applicability: All	References: ARS: MA-CMS-1(CMS-0); HIPAA: 164.310(d)(2)(i)	Related Controls:	
ASSESSMENT PROCEDURE: MA-CMS-1(CN	S-0).1		
Assessment Objective			
Determine if the organization allows only author	zed personnel perform maintenance on the information system.		
Assessment Methods And Objects			
Examine: Information system maintenance poli		t only authorized personnel are permitted access to the system for repair. by authorized personnel. After maintenance is performed, security features	
are checked to verify they are functioning prope			
		personnel are permitted access to system for repair. Storage media must be	
	storage media must be degaussed or destroyed by authorized personne	I. After maintenance is performed, security features are checked to verify	
they are functioning properly. IA-CMS-2 – On-site Physical Repair of Systems (Low)			
	Systems (Low)		
Control		a second and the second second	
	mplemented effectively to enable on-site physical repair of systems witho	but compromising security functionality or confidentiality.	
Guidance		considered as a size. The second events as should reach the second Observe	
Management baseline.	aw of a system before it is put back into operation when the system has o	completed repairs. The repaired system should match the approved Change	
Storage media control when encrypted may take	special considerations.		
Applicability: All	References: ARS: MA-CMS-2; PISP: 4.9.8	Related Controls: AC-19(CMS-1), AC-3,	
		CP-9, SC-12(CMS-1)	
ASSESSMENT PROCEDURE: MA-CMS-2.1			
Assessment Objective			
Determine if the organization effectively develop	s procedures, documents procedures, and implements on-site repair of s	systems without compromising security functionality or confidentiality.	
Assessment Methods And Objects			
Examine: Information system maintenance polic repair.	y and procedures; other relevant documents or records to determine that	t only authorized personnel are permitted access to the system for on-site	
Interview: Organizational personnel with inform	ation system maintenance responsibilities to determine that only authoriz	ed personnel are permitted access to systems during on-site repair.	
MA-CMS-2(CMS-1) – Enhancement (Low)			
Control			
Access to system for repair must be by authoriz	ed personnel only.		
Applicability: All	References: ARS: MA-CMS-2(CMS-1)	Related Controls:	
ASSESSMENT PROCEDURE: MA-CMS-2(CM			
Assessment Objective	· ·		
	zed personnel perform maintenance on the information system.		
	· · · · · · · · · · · · · · · · · · ·		

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records to determine physical repair of servers is performed within protected environments. **Interview:** Organizational personnel with information system maintenance responsibilities to determine physical repair of servers is performed within protected environments.

Media Protection (MP) – Operational

MP-1 – Media Protection Policy and Procedures (Low) Control MP controls and procedures shall be developed, documented, and implemented effectively to address media access; media labeling; media transport; media destruction; media sanitization and clearing: media storage; and disposition of media records. The MP procedures shall be consistent with applicable laws. Executive Orders, directives, policies, regulations, standards, and guidance. Guidance The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. Applicability: All References: ARS: MP-1; FISCAM: TAC-3.4; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1; NIST 800-**Related Controls:** 53/53A: MP-1: PISP: 4.10.1 ASSESSMENT PROCEDURE: MP-1.1 **Assessment Objective** Determine if: (i) the organization develops and documents media protection policy and procedures; (ii) the organization disseminates media protection policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review media protection policy and procedures; and (iv) the organization updates media protection policy and procedures when organizational review indicates updates are required. Assessment Methods And Objects Examine: Media protection policy and procedures; other relevant documents or records. Interview: Organizational personnel with information system media protection responsibilities. (Optional) **ASSESSMENT PROCEDURE: MP-1.2 Assessment Objective** Determine if: (i) the media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance: (ii) the media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated security controls. Assessment Methods And Objects Examine: Media protection policy and procedures; other relevant documents or records. Interview: Organizational personnel with information system media protection responsibilities.(Optional) MP-2 – Media Access (Low) Control Procedures shall be developed, documented, and implemented effectively to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media based on the sensitivity of the CMS information. Automated mechanisms shall be implemented to control access to media storage areas and to audit access attempts and access granted. Guidance Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). An organizational assessment of risk guides the selection of media and associated information contained on that media reguiring restricted access. Organizations document in policy and procedures. the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. Applicability: All References: ARS: MP-2; FISCAM: TAC-3.1.A.6, TAY-4.1.1; HIPAA: 164.308(a)(3)(ii)(A), Related Controls: 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1; NIST 800-53/53A: MP-2; PISP: 4.10.2

ASSESSMENT PROCEDURE: MP-2.1

Assessment Objective

Determine if the organization restricts access to information system media to authorized users.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records.

Interview: Organizational personnel with information system media protection responsibilities.(Optional)

MP-4 – Media Storage (Low)

Control

Media storage procedures shall be developed, documented, and implemented effectively to facilitate the secure storage of media, both electronic and paper, within controlled areas. Storage media shall be controlled physically and safeguarded in the manner prescribed for the highest system security level of the information ever recorded on it until destroyed or sanitized using CMS-approved procedures.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management.

Applicability: All	References: ARS: MP-4; FISCAM: TCC-3.2.4, TCC-3.3.1; IRS-1075: 4.6#1, 4.6#3, 5.3#1, 6.3.2#1; NIST 800-53/53A: MP-4; PISP: 4.10.4	Related Controls: AC-19, CP-9, CP-9(4), RA-2, SC-7

ASSESSMENT PROCEDURE: MP-4.1

Assessment Objective

Determine if:

(i) the organization defines controlled areas for information system media;

(ii) the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk;

(iii) the organization defines the specific measures used to protect the selected media and information contained on that media;

(iv) the organization physically controls and securely stores information system media within controlled areas; and

(v) the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media; other relevant documents or records.(Optional)

MP-6 – Media Sanitization and Disposal (Low)

Control

Formal documented procedures shall be developed and implemented effectively to ensure that sanitization and disposal methods are commensurate with the sensitivity and criticality of data residing on storage devices, equipment, and hard copy documents. Media sanitization actions shall be tracked, documented, and verified. Sanitization equipment and procedures shall be tested periodically to ensure proper functionality.

Media destruction and disposal procedures shall be developed, documented, and implemented effectively, in an environmentally approved manner, to facilitate the disposal of media, both electronic

and paper using approved methods, to ensure that CMS information does not become available to unauthorized personnel. Approved equipment removal procedures for CMS information systems and components that have processed or contained CMS information shall be followed. Inventory and disposition records for media, both electronic and paper, shall be produced, stored, updated, and retained.

Guidance

Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

		J J J J J J J J J J J J J J J J J J J	
App	olicability: All	References: ARS: MP-6; FISCAM: TAC-3.4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-1075:	Related Controls: MA-4
	-	4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2; NIST 800-53/53A: MP-6; PISP: 4.10.6	

ASSESSMENT PROCEDURE: MP-6.1

Assessment Objective

Determine if:

(i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process;

(ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and

(iii) information system media sanitation is consistent with NIST SP 800-88.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST SP 800-88; media sanitization records; audit records; other relevant documents or records.

Interview: Organizational personnel with information system media sanitization responsibilities.(Optional)

Physical and Environmental Protection (PE) – Operational

PE-1 – Physical and Environ	mental Protection Policy and Procedures (Low)	
Control		
	ection procedures shall be developed and implemented effectively to protect all CN	MS IT infrastructure and assets from unauthorized access, disclosure, duplication,
	on, loss, misuse, or theft whether accidental or intentional. These procedures shall	
	directives, regulations, and guidelines.	
Guidance		
	protection policy and procedures are consistent with applicable laws. Executive Or	rders, directives, policies, regulations, standards, and guidance. The physical and
	an be included as part of the general information security policy for the organization	
	for a particular information system, when required. NIST SP 800-12 provides guid	
Applicability: All	References: ARS: PE-1; FISCAM: TSC-2.2.6, TSC-2.3.4, TSD-2 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1; NIST 800-53/5	
ASSESSMENT PROCEDURE: P	E-1.1	
Assessment Objective		
Determine if:		
	documents physical and environmental protection policy and procedures;	
	physical and environmental protection policy and procedures to appropriate elem	
	organization periodically review physical and environmental protection policy and	
	sical and environmental protection policy and procedures when organizational rev	view indicates updates are required.
Assessment Methods And Obje		
	nental protection policy and procedures; other relevant documents or records.	
¥i	nel with physical and environmental protection responsibilities.(Optional)	
ASSESSMENT PROCEDURE: P	E-1.2	
Assessment Objective		
Determine if:		
	al protection policy addresses purpose, scope, roles and responsibilities, managen	
		with applicable laws, directives, policies, regulations, standards, and guidance; and
	al protection procedures address all areas identified in the physical and environme	ental protection policy and address achieving policy-compliant implementations of
all associated security controls.		
Assessment Methods And Obje		
	nental protection policy and procedures; other relevant documents or records. nel with physical and environmental protection responsibilities.(Optional)	
PE-1(FIS-1) – Enhancement (Lo		
Control	w)	
	ior that may damage computer equipment is prohibited.	
Applicability: All	References: FISCAM: TSC-2.2.7	Related Controls:
ASSESSMENT PROCEDURE: P		
Assessment Objective		
	hibits eating, drinking, and other behavior that may damage computer equipment.	
Assessment Methods And Obje		
Examine: Employee behavior.	5010 	
Examine: Employee behavior. Examine: Employee rules of bel	navior	
Examine: Pertinent policies and		
Interview: Information system m	1	

	$\rho \rightarrow \lambda$	
PE-2 – Physical Access Authorizations	(LOW)	
Control		
shall be documented on standard forms, mainta	s to facilities containing CMS information or information systems (except for those areas within the facilitie ined on file, approved by appropriate organizational officials, and reviewed periodically, and, if necessary mart cards) shall be issued to authorized personnel. Personnel who no longer require access shall be re	, updated. Appropriate authorization
Guidance		
Appropriate authorization credentials include, for to the facility where the information system resident	or example, badges, identification cards, and smart cards. The organization promptly removes from the ac des.	ccess list personnel no longer requiring access
Applicability: All	References: ARS: PE-2; FISCAM: TAC-2.1.1, TAC-2.1.2, TAC-2.1.4, TAC-2.2, TAC-3.1.A.3, TAC-3.1.A.4, TAC-3.1.A.8, TSS-1.2.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	Related Controls:
ASSESSMENT PROCEDURE: PE-2.1		
 (iii) the organization develops and keeps current designated as publicly accessible); (iv) the organization issues appropriate authoriz (v) designated officials within the organization responses to the term of te	cility that are publicly accessible; riew and approval for the physical access list and authorization credentials for the facility; t lists of personnel with authorized access to the facility where the information system resides (except for ration credentials (e.g., badges, identification cards, smart cards); and eview and approve the access list and authorization credentials at the organization-defined frequency, at an policy; procedures addressing physical access authorizations; authorized personnel access list; authori	least annually.
Control		
	norized access to facilities containing information systems at least once every 365 days.	
Applicability: All	References: ARS: PE-2(0); FISCAM: TAC-2.1.2, TAC-2.1.4, TAC-3.1.A.4; NIST 800-53/53A: PE-2; PISP: 4.11.2	Related Controls:
ASSESSMENT PROCEDURE: PE-2(0).1		
Assessment Methods And Objects	ments as specified in the baseline control and the specific CMS requirements as prescribed in this amplify on policy; procedures addressing physical access authorizations; authorized personnel access list; authori	
PE-3 – Physical Access Control (Low)		
Control Physical access control devices (e.g., keys, lock systems, except for areas and/or facilities officia	ks, combinations, card-readers) and/or guards shall be used to control entry to and exit from facilities con- ally designated as publicly accessible. Individual access authorizations shall be verified before granting a ol devices (e.g., keys, locks, combinations, key cards) shall be secured and inventoried on a regular basis	ccess to facilities containing CMS information
	changed promptly when lost, compromised, or when individuals are transferred or terminated. Re-entry Access to workstations and associated peripheral computing devices shall be appropriately controlled v	
Guidance		
keys, combinations, and other access devices a compromised, or individuals are transferred or t designated as publicly accessible with access to	(e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing inform and inventories those devices regularly. The organization changes combinations and keys: (i) periodically, erminated. Workstations and associated peripherals connected to (and part of) an organizational informa o such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credentia control system conforms to the requirements of FIPS 201 and NIST SP 800-73. If the token-based access	; and (ii) when keys are lost, combinations are tion system may be located in areas al is used as an identification token and token-

Rev. 9

to the requirements of NIST SP 800-	m conforms to the requirements of NIST SP 800-78. If the token-based access control function employs biometric ve .76.	erification, the access control system conform
Applicability: All	References: ARS: PE-3; FISCAM: TAC-3.1.A.3, TAC-3.1.A.5, TAC-3.1.A.7, TAC-3.1.A.8, TAC- 3.1.B.2, TAN-2.1.1, TAN-2.1.2, TAN-2.2.1, TSD-2.1; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1; NIST 800-53/53A: PE-3; PISP: 4.11.3	Related Controls:
SSESSMENT PROCEDURE: PE-3	.1	
ssessment Objective		
designated as publicly accessible);	cal access points (including designated entry/exit points) to the facility where the information system resides (except	for those areas within the facility officially
()	cess to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's asse	ssment of risk.
ssessment Methods And Objects		
	tal protection policy; procedures addressing physical access control; physical access control logs or records; other re with physical access control responsibilities.(Optional) ility (Optional)	elevant documents or records.
ASSESSMENT PROCEDURE: PE-3		
ssessment Objective		
Determine if: (i) physical access devices (e.g., key (ii) the organization secures keys, co (iii) keys and combinations to locks v	rs, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a re ombinations and other access devices on a regular basis; and vithin the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are to	
ssessment Methods And Objects		
	tal protection policy; procedures addressing physical access control; physical access control logs or records; mainte ons for keys and access devices; other relevant documents or records.	nance records; records of key and lock
Test: Physical access control device		
ASSESSMENT PROCEDURE: PE-3		
Assessment Objective	-	
Determine if:		
(i) the access control system is cons access control is employed);	istent with FIPS 201 and NIST SP 800-73 (where the federal Personal Identity Verification (PIV) credential is used a	s an identification token and token-based
	sistent with NIST SP 800-78 (where the token-based access control function employs cryptographic verification); and	Ł
	sistent with NIST SP 800-76 (where the token-based access control function employs biometric verification).	
ssessment Methods And Objects		
other relevant documents or records		8; information system design documentation
Test: Physical access control device		
PE-3(CMS-1) – Enhancement (Low		
Control		
Control data center / facility access b		
pplicability: All	References: ARS: PE-3(CMS-1); IRS-1075: 4.6#1	Related Controls:
SSESSMENT PROCEDURE: PE-3	(CMS-1).1	
officially designated as publicly acce		es (except for those areas within the facility
Assessment Methods And Objects		
	al protection policy; procedures addressing physical access control; physical access control logs or records; other re Iled by use of door and window locks.	elevant documents or records to determine
Rev. 9	Page 75 of 127	BPSSM Appendix A. Attachmer

. .

م ما 4

Interview: Organizational personnel with phy	vsical access control responsibilities to confirm data center / facility access is controlled	t by use of door and wi	indow locks
PE-3(CMS-2) – Enhancement (Low)			
Control			
	re environments protected from unauthorized access.		
Applicability: All	References: ARS: PE-3(CMS-2); FISCAM: TAC-3.1.A.5; IRS-1075: 4.6#1		Related Controls:
ASSESSMENT PROCEDURE: PE-3(CMS-2		ļ	Trefated Controls.
Assessment Objective	•/•		
Determine if the organization controls all physical	visical access points (including designated entry/exit points) to the facility where the infor	rmation system resides	s (except for those areas within the facility
officially designated as publicly accessible). Assessment Methods And Objects			
Examine: Physical and environmental protect	ction policy; procedures addressing physical access control; physical access control log	gs or records; other rel	evant documents or records to determine
	vsical access control responsibilities to determine servers are stored and operated in ph	hysically secure enviro	pmonte protoctod from upputhorized access
PE-3(CMS-3) – Enhancement (Low)	vsical access control responsibilities to determine servers are stored and operated in pr	Tysically secure enviro	niments protected from driadtronzed access:
Control			
-	ements as established by the Federal Information Systems Control Audit Manual (FISC		
Applicability: All	References: ARS: PE-3(CMS-3); FISCAM: TAC-3.1.A.1, TAN-2.1.1, TAN-2.1.2; I	RS-1075: 4.6#1	Related Controls:
ASSESSMENT PROCEDURE: PE-3(CMS-3	3).1		
Assessment Objective			
Determine if:			
	ss points (including designated entry/exit points) to the facility where the information sys	stem resides (except for	or those areas within the facility officially
designated as publicly accessible);			
(ii) the organization verifies individual access	authorizations before granting access to the facility; and		
(iii) the organization also controls access to a	areas officially designated as publicly accessible, as appropriate, in accordance with the	e organization's assess	sment of risk.
Assessment Methods And Objects			
	ction policy; procedures addressing physical access control; physical access control log s as established by the Federal Information Systems Control Audit Manual (FISCAM).	gs or records; other rel	evant documents or records to determine if
PE-3(DIR-1) – Enhancement (Low)			
Control			
Controls are established to protect access at	uthorization lists to secure areas such as data centers.		
Applicability: All	References:		Related Controls:
ASSESSMENT PROCEDURE: PE-3(DIR-1)			
Assessment Objective			
•	ved access authorization lists that are for secure areas.		
Assessment Methods And Objects			
···· , ···			
PE-4 – Access Control for Transmiss	e for approved access authorization lists to secure areas.		
Control			
	, documented, and implemented effectively to protect against eavesdropping, in-transit	modification disruption	n and/or physical tamporing of CMS
	organizational facilities that carry unencrypted information.	mounication, disruption	n, and/or physical tampening of CMS
Guidance	organizational radinado ana darry anonorypica information.		
	ystem distribution and transmission lines help prevent accidental damage, disruption, a	nd physical tomporing	Additionally physical protections are
necessary to belo prevent eavesdropping or	in transit modification of unencrypted transmissions. Protective measures to control phy	nu priysical tampering.	ation system distribution and transmission
lines include: (i) locked wiring closets: (ii) dis	connected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable tra	ysicai access io inionn avs	auon system uismbution anu transmission
Applicability: All	References: ARS: PE-4; FISCAM: TAC-3.2.E.1; NIST 800-53/53A: PE-4; PISP: 4		
		1114	Related Controls:

ASSESSMENT PROCEDURE: PE-4.1			
Assessment Objective			
Determine if the organization controls physical a	ccess to information system distribution and transmission lines within organizational facilities.		
Assessment Methods And Objects			
Examine: Physical and environmental protection	n policy; procedures addressing access control for transmission medium; information system design do	ocumentation; facility communications and wirin	
diagrams; other relevant documents or records.	(Optional)		
PE-4(CMS-1) – Enhancement (Low)			
Control			
Prohibit public access to telephone closets and i	information system distribution and transmission lines within organizational facilities.		
Applicability: All	References: ARS: PE-4(CMS-1); FISCAM: TAC-3.2.E.1	Related Controls:	
ASSESSMENT PROCEDURE: PE-4(CMS-1).1			
Assessment Objective			
	access to information system distribution and transmission lines within organizational facilities.		
Assessment Methods And Objects			
•	n policy; procedures addressing physical access control; physical access control logs or records; other	relevant documents or records to determine if	
	tem distribution and transmission lines within organizational facilities are restricted only to authorized p		
	al access control responsibilities to determine if access to telephone closets and information system di	stribution and transmission lines within	
organizational facilities are restricted only to aut	horized personnel.		
PE-4(CMS-2) – Enhancement (Low)			
Control			
Disable any physical ports (e.g., wiring closets,	patch panels, etc) not in use.		
Applicability: All	References: ARS: PE-4(CMS-2)	Related Controls:	
ASSESSMENT PROCEDURE: PE-4(CMS-2).1			
Assessment Objective			
Determine if the organization controls physical a	access to information system distribution and transmission lines within organizational facilities.		
Assessment Methods And Objects	,		
Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring			
•	n policy; procedures addressing access control for transmission medium; information system design do	ocumentation; facility communications and wirin	
Examine: Physical and environmental protection diagrams; other relevant documents or records t	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled.	· · · ·	
Examine: Physical and environmental protection diagrams; other relevant documents or records t Interview: Organizational personnel with physic	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. al access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et	· · · ·	
Examine: Physical and environmental protection diagrams; other relevant documents or records t	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. al access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et		
Examine: Physical and environmental protection diagrams; other relevant documents or records t Interview: Organizational personnel with physic	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. al access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et	· · · ·	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physical PE-6 – Monitoring Physical Access (Lo Control	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. al access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et	c) not in use are disabled.	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physic PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. al access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w)	c) not in use are disabled.	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physical PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. al access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ	c) not in use are disabled.	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physic PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vio Guidance	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. al access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ	c) not in use are disabled. ization officials shall periodically review physica	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physic PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vio Guidance	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. tal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondent	c) not in use are disabled. ization officials shall periodically review physica	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physical PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vio Guidance The organization reviews physical access logs p	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. tal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondibility. References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN-	c) not in use are disabled. ization officials shall periodically review physica	
 Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physical PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vide Guidance The organization reviews physical access logs part of the organization's incident response capa Applicability: All 	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. tal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondibility.	c) not in use are disabled. ization officials shall periodically review physica	
 Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physical PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vide Guidance The organization reviews physical access logs part of the organization's incident response capa Applicability: All 	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. tal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondibility. References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN-	c) not in use are disabled. ization officials shall periodically review physica	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physic PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vio Guidance The organization reviews physical access logs p part of the organization's incident response capa Applicability: All ASSESSMENT PROCEDURE: PE-6.1 Assessment Objective	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. cal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondentiate ability. References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN- 2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6	c) not in use are disabled. ization officials shall periodically review physica	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physic PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vio Guidance The organization reviews physical access logs p part of the organization's incident response capa Applicability: All ASSESSMENT PROCEDURE: PE-6.1 Assessment Objective Determine if the organization monitors physical access and applicability of the organization for the organizatio	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. tal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondibility. References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN-	c) not in use are disabled. ization officials shall periodically review physica	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physic PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vio Guidance The organization reviews physical access logs p part of the organization's incident response capa Applicability: All ASSESSMENT PROCEDURE: PE-6.1 Assessment Objective Determine if the organization monitors physical access and the organization monitors physical access access and the organization monitors physical access a	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. tal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondability. References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN- 2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6 access to the information system to detect and respond to physical security incidents.	c) not in use are disabled. ization officials shall periodically review physica onse to detected physical security incidents is Related Controls: IR-4	
 Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physic PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vid Guidance The organization reviews physical access logs p part of the organization's incident response capa Applicability: All ASSESSMENT PROCEDURE: PE-6.1 Assessment Objective Determine if the organization monitors physical access 	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. cal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondability. References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN- 2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6 access to the information system to detect and respond to physical security incidents. n policy; procedures addressing physical access monitoring; physical access logs or records; other relevance.	c) not in use are disabled. ization officials shall periodically review physica onse to detected physical security incidents is Related Controls: IR-4	
Examine: Physical and environmental protection diagrams; other relevant documents or records to Interview: Organizational personnel with physic PE-6 – Monitoring Physical Access (Lo Control Physical access to information systems shall be access records, investigate apparent security vid Guidance The organization reviews physical access logs p part of the organization's incident response capa Applicability: All ASSESSMENT PROCEDURE: PE-6.1 Assessment Objective Determine if the organization monitors physical a Assessment Methods And Objects	to determine if all physical ports (e.g., wiring closets, patch panels, etc) not in use are disabled. cal access control responsibilities to determine if all physical ports (e.g., wiring closets, patch panels, et w) monitored for physical security compliance and to detect and respond to incidents. Appropriate organ olations or suspicious physical access activities, and take appropriate remedial action. periodically and investigates apparent security violations or suspicious physical access activities. Respondability. References: ARS: PE-6; FISCAM: TAC-4.2, TAC-4.3.1, TAC-4.3.2, TAC-4.3.4, TAN-2.1.1, TAN- 2.1.2; NIST 800-53/53A: PE-6; PISP: 4.11.6 access to the information system to detect and respond to physical security incidents. n policy; procedures addressing physical access monitoring; physical access logs or records; other releval access monitoring responsibilities.(Optional)	c) not in use are disabled. ization officials shall periodically review physica onse to detected physical security incidents is Related Controls: IR-4	

PE-7 – Visitor Control (Low)				
Control				
	and implemented effectively to control access to sensitive facilities and restricted / controlled areas control			
	and media libraries. Visitors shall be authenticated prior to being granted access to facilities or areas other than areas designated as publicly accessible. Government contractors and others with			
permanent authorization credentials are not cons	sidered visitors.			
Guidance				
	ent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials f	or federal employees and contractors		
	ns for the PIV credentials are accredited in accordance with the provisions of NIST SP 800-79.			
Applicability: All	References: ARS: PE-7; FISCAM: TAC-3.1.B.3; HIPAA: 164.310(a)(2)(iii); NIST 800-53/53A: PE-7; PISP: 4.11.7	Related Controls:		
ASSESSMENT PROCEDURE: PE-7.1				
Assessment Objective				
	ccess to the information system by authenticating visitors before authorizing access to the facility where	the information system resides other than		
areas designated as publicly accessible.		the information system resides other than		
Assessment Methods And Objects				
	policy; procedures addressing visitor access control; visitor access control logs or records; other releva	nt documents or records		
Interview: Organizational personnel with visitor		in documents of records.		
Test: Visitor access control capability.(Optional)				
PE-7(FIS-1) – Enhancement (Low)				
Control				
	l are authenticated through the use of preplanned appointments and identification checks.			
Applicability: All	References: FISCAM: TAC-3.1.B.3	Related Controls:		
ASSESSMENT PROCEDURE: PE-7(FIS-1).1				
Assessment Objective				
•	rs, contractors and maintenance personnel through the use of preplanned appointments and identification	n checks		
•				
Assessment Methods And Objects				
Examine: Appointment and verification procedures for visitors. Examine: Pertinent policies and procedures.				
Interview: Receptionist or security guard.				
PE-8 – Access Records (Low)				
Control	I / controlled erece that contain CMC information or information systems shall be leaged. The visitor and	and record shall contain.		
4.11.8.1. Name and organization of the person v	I / controlled areas that contain CMS information or information systems shall be logged. The visitor acc isiting:	ess record shall contain.		
4.11.8.2. Signature of the visitor;	isung,			
4.11.8.3. Form of identification;				
4.11.8.4. Date of access;				
4.11.8.5. Time of entry and departure;				
4.11.8.6. Purpose of visit; and				
4.11.8.7. Name and organization of person visite	d.			
Appropriate organization officials shall periodical	ly review the access records, including after closeout.			
Guidance	y review the access records, including after closeout.			
	for consistency and ease of use during log closeouts and the next months log generation.			
Applicability: All	References: ARS: PE-8; FISCAM: TAC-3.1.B.1, TAC-3.1.B.3; NIST 800-53/53A: PE-8; PISP: 4.11.8	Related Controls:		
ASSESSMENT PROCEDURE: PE-8.1				
Assessment Objective				
Determine if:				

(i) the organization defines the frequency of review for visitor access records: (ii) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: - name and organization of the person visiting; - signature of the visitor; - form of identification; - date of access: - time of entry and departure; - purpose of visit; - name and organization of person visited and (iii) designated officials within the organization review the visitor access logs in accordance with organization-defined frequency. Assessment Methods And Objects Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan; facility access control records; other relevant documents or records. PE-8(0) – Enhancement (Low) Control Visitor access records must be closed out and reviewed by management monthly. Applicability: All References: ARS: PE-8(0); NIST 800-53/53A: PE-8; PISP: 4.11.8 **Related Controls:** ASSESSMENT PROCEDURE: PE-8(0).1 **Assessment Objective** Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan (for organization-defined frequency for review of visitor access records); facility access control records; other relevant documents or records. PE-9 – Power Equipment and Power Cabling (Low) Control Power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to maintain safe power for CMS information systems. Guidance Both primary and backup power systems should be included in the safe power implementation procedures. Remote backup site's power implementation should be included in the documentation. References: ARS: PE-9; NIST 800-53/53A: PE-9; PISP: 4.11.9 **Related Controls:** Applicability: All ASSESSMENT PROCEDURE: PE-9.1 Assessment Objective Determine if the organization protects power equipment and power cabling for the information system from damage and destruction. **Assessment Methods And Objects** Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.(Optional) PE-9(CMS-1) – Enhancement (Low) Control Prohibit public access to infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets. References: ARS: PE-9(CMS-1) Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: PE-9(CMS-1).1 **Assessment Objective** Determine if the organization protects power equipment and power cabling for the information system from damage and destruction. **Assessment Methods And Objects** Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets. Interview: Organizational personnel with physical access control responsibilities to determine if only authorized maintenance personnel are permitted to access infrastructure assets, including power

generators, HVAC systems, cabling, and wiring closets. PE-9(CMS-2) – Enhancement (Low) Control Power surge protection must be implemented for all computer equipment. Applicability: All References: ARS: PE-9(CMS-2) **Related Controls:** ASSESSMENT PROCEDURE: PE-9(CMS-2).1 **Assessment Objective** Determine if the organization protects power equipment and implements surge protection for all computers to assist in protection from damage or destruction. **Assessment Methods And Objects** Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents /records / diagrams to determine if power surge protection is implemented for all computer equipment. Interview: Organizational personnel with physical access control responsibilities to determine if power surge protection is implemented for all computer equipment. PE-11 – Emergency Power (Low) Control Emergency power supply control mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to facilitate an orderly shutdown of the CMS information system in the event of a primary power source loss. Guidance Both primary and backup processing locations should be included in the safe power implementation procedures. The remote backup site's power implementation should be included in the documentation. Even though unlikely that both the primary and backup locations will be switching to emergency power at the same time, it is prudent to minimize the risk to a total lose of a processing capability. Applicability: All References: ARS: PE-11: FISCAM: TSC-2.2.5: NIST 800-53/53A: PE-11: PISP: 4.11.11 **Related Controls: ASSESSMENT PROCEDURE: PE-11.1 Assessment Objective** Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. Assessment Methods And Objects Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records.(Optional) Test: Uninterruptible power supply.(Optional) PE-12 – Emergency Lighting (Low) Control Mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to enhance safety and availability. Automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes shall be provided. Guidance Local building safety codes are a good place to obtain the needed information for documenting emergency lighting implementation procedures and architecture. References: ARS: PE-12: NIST 800-53/53A: PE-12: PISP: 4.11.12 **Related Controls:** Applicability: All **ASSESSMENT PROCEDURE: PE-12.1** Assessment Objective Determine if: (i) the organization employs and maintains automatic emergency lighting systems that activates in the event of a power outage or disruption; and (ii) the organization employs and maintains automatic emergency lighting systems that cover emergency exits and evacuation routes. **Assessment Methods And Objects** Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records. Test: Emergency lighting capability.(Optional) PE-13 – Fire Protection (Low) Control Fire protection mechanisms shall be in place and supporting procedures shall be developed, documented, and implemented effectively to prevent, detect, and respond to fire. Fire suppression and

detection devices / systems that can be activate sprinkler systems, hand-held fire extinguishers, f	d in the event of a fire shall be employed and maintained. Fire suppression and detection devices / s ixed fire hoses, and smoke detectors.	ystems shall include, but not be limited to,		
Guidance				
Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.				
Applicability: All	References: ARS: PE-13; FISCAM: TSC-2.2.1, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-13; PISP: 4.11.13	Related Controls:		
ASSESSMENT PROCEDURE: PE-13.1				
Assessment Objective				
	ains fire suppression and detection devices/systems that can be activated in the event of a fire.			
Assessment Methods And Objects				
documentation; test records of fire suppression a	n policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire s and detection devices/systems; other relevant documents or records.	uppression and detection devices/systems		
PE-14 – Temperature and Humidity Con-	trols (Low)			
Control				
Temperature and humidity control mechanisms monitor the temperature and humidity of facilities	shall be in place and supporting procedures shall be developed, documented, and implemented effects containing CMS information systems.	tively to maintain (within acceptable levels) and		
Guidance				
Local building a safety codes are a good place to Health Administration (OSHA) requirements may	o obtain the needed information for documenting HVAC implementation procedures and architecture. /be included.	Consideration for Occupational Safety and		
Applicability: All	References: ARS: PE-14; FISCAM: TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-14; PISP: 4.11.1	4 Related Controls:		
ASSESSMENT PROCEDURE: PE-14.1				
Assessment Objective Determine if: (i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and (ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides; and (ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides; and (iii) the organization regularly monitors the temperature and humidity within the facility where the information system resides; Assessment Methods And Objects Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity records; other relevant documents or records.				
PE-14(CMS-1) – Enhancement (Low)				
Control	nuidelines for that short lovel			
Evaluate the level of alert and follow prescribed Applicability: All	References: ARS: PE-14(CMS-1)	Related Controls:		
ASSESSMENT PROCEDURE: PE-14(CMS-1).		Related Controls.		
Assessment Objective Determine if: (i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and (ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides; and (ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides; and (ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides; and (ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides. Assessment Methods And Objects Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity records; other relevant documents or records to determine the level of alert and prescribed guidelines for that alert level. Interview: Organizational personnel with environmental protection responsibilities to determine if there exists the level of alert and prescribed guidelines for that alert level. PE-14(FIS-1) – Enhancement (Low) Control Redundancy exists in the air cooling system.				
Applicability: All	References: FISCAM: TSC-2.2.3	Related Controls:		

ASSESSMENT PROCEDURE: PE-14(FIS-1).1					
Assessment Objective					
Determine if the organization uses redundant air	r cooling systems				
Assessment Methods And Objects					
Examine: Entity's facilities. Examine: Operation, location, maintenance, and access to the air cooling systems.					
Examine: Operation, location, maintenance, and access to the air cooling systems. Examine: Pertinent policies and procedures.					
Examine: Pertinent policies and procedures. Interview: Site manager.					
PE-15 – Water Damage Protection (Low	()				
Control					
	t the building plumbing does not endanger CMS information systems. Procedures shall be developed, d s.	ocumented, and implemented effectively to			
Guidance					
	o obtain the needed information for documenting water damage protection procedures and architecture. /be included.	Consideration for Occupational Safety and			
Applicability: All	References: ARS: PE-15; FISCAM: TSC-2.2.4, TSC-2.3.2, TSC-2.3.3; NIST 800-53/53A: PE-15; PISP: 4.11.15	Related Controls:			
ASSESSMENT PROCEDURE: PE-15.1					
Assessment Objective					
Determine if:					
	knowledge of location and operational procedures for activating master shutoff valves for plumbing syst	em; and			
(ii) the organization protects the information syst	em from water damage resulting from broken plumbing lines or other sources of water leakage by provi	-			
working properly, and known to key personnel.					
Assessment Methods And Objects					
knowledge of location and activation procedures	n policy; procedures addressing water damage protection; facility housing the information system; master for master shutoff values for the plumbing system; master shutoff value documentation; other relevant				
	and environmental protection responsibilities.(Optional)				
	Test: Simulated master water shutoff value activation for the plumbing system.(Optional)				
PE-16 – Delivery and Removal (Low)					
Control					
Procedures shall be developed, documented, and implemented effectively to control the flow of information system-related items into and out of the organization. Appropriate officials shall authorize the delivery or removal of CMS information system-related items.					
To avoid unauthorized access, delivery and removal controls shall be implemented to isolate delivery areas from sensitive facilities and restricted / controlled areas containing CMS information, information systems, and media libraries.					
Guidance					
The organization controls delivery areas and, if	possible, isolates the areas from the information system and media libraries to avoid unauthorized physi	cal access.			
Applicability: All	References: ARS: PE-16; NIST 800-53/53A: PE-16; PISP: 4.11.16	Related Controls:			
ASSESSMENT PROCEDURE: PE-16.1					
Assessment Objective					
Determine if:					
	related items (i.e., hardware, firmware, software) entering and exiting the facility; and				
(ii) the organization maintains appropriate record	as or items entering and exiting the facility.				
Assessment Methods And Objects	n i in in i i i i i i i i i i i i i i i				
Examine: Physical and environmental protection records of items entering and exiting the facility;	 policy; procedures addressing delivery and removal of information system components from the facility other relevant documents or records. 	r; racility housing the information system;			
o o i	responsibilities for information system components entering and exiting the facility.(Optional)				
Pay 0	Page 82 of 127	BDSSM Appendix A Attachment 3			

PE-17 – Alternate Work Site (Low)

Control

Procedures shall be developed, documented, and implemented effectively to control information system security at alternate work sites. A method of communication shall be provided to employees at alternate work sites to report security issues or suspected security incidents.

Guidance

The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST SP 800-46 provides guidance on security in telecommuting and broadband communications.

Applicability: All	References: ARS: PE-17; HIPAA: 164.310(a)(2)(i); NIST 800-53/53A: PE-17; PISP: 4.11.17	Related Controls:
ASSESSMENT PROCEDURE: PE-17.1		

Assessment Objective

Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant documents or records.(Optional)

Interview: Organization personnel using alternate work sites.(Optional)

Planning (PL) – Management

PL-1 – Security Planning Policy and Procedures (Low)

Control

All CMS information systems and major applications shall be documented in a SSP, which is compliant with OMB Circular A-130 and consistent with NIST SP 800-18. The SSP shall be approved by appropriate organization officials and incorporated into the information resources management strategic plan. The information contained in the SSP is the basis for system accreditation, and subject to reporting requirements as established by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, in accordance with current CMS Procedures.

Guidance

The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-18 provides guidance on security planning. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All References: ARS: PL-1; FISCAM: TSP-2.1, TSP-3.2; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2; NIST 800-53/53A: PL-1; PISP: 4.12.1 Related Controls:

ASSESSMENT PROCEDURE: PL-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents security planning policy and procedures;

(ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review security planning policy and procedures; and

(iv) the organization updates security planning policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

ASSESSMENT PROCEDURE: PL-1.2

Assessment Objective

Determine if:

(i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.

Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

References: FISCAM: TSP-3.3.2

PL-1(FIS-1) – Enhancement (Low)

Control

Security policies are distributed to all affected personnel.

Applicability: All

ASSESSMENT PROCEDURE: PL-1(FIS-1).1

Assessment Objective

Determine if the organization distributes security policies to all affected personnel.

Assessment Methods And Objects

Examine: Memos, electronic mail files, or other policy distribution mechanisms.

Interview: Staff and system users to determine how security policies are distributed.

PL-2 – System Security Plan (SSP) (Low)

Control

All CMS information systems and major applications shall be covered by an SSP, which is compliant with OMB Circular A-130 and consistent with the intent of NIST SP 800-18. The SSP shall document the operation and security requirements of the system / application and the controls in place for meeting those requirements. The SSP shall be approved by appropriate organization

Related Controls:

officials and incorporated into the information res Executive Orders, directives, policies, regulation	sources management strategic plan. The information contained in the SSP is subject to reporting require s, standards, and guidance, including, but not limited to, current CMS Procedures.	ments as established by applicable laws,		
Guidance				
The security plan is aligned with the organization	n's information system architecture and information security architecture. NIST SP 800-18 provides guida	nce on security planning.		
Applicability: All	References: ARS: PL-2; FISCAM: TAC-3.1.A.1, TSP-2.1, TSP-3.2; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3; NIST 800-53/53A: PL-2; PISP: 4.12.2	Related Controls:		
ASSESSMENT PROCEDURE: PL-2.1				
Assessment Objective				
Determine if:				
(i) the organization develops and implements a s	security plan for the information system;			
	security requirements for the information system and a description of the security controls planned or in with NIST SP 800-18 and the concepts in the NIST Risk Management Framework including baseline secu			
(iv) the security plan is consistent with the organ	ization's information system architecture and information security architecture; and			
(v) designated organizational officials review and				
Assessment Methods And Objects				
Examine: Security planning policy; procedures a relevant documents or records.	addressing information system security plan development and implementation; NIST SP 800-18; security	plan for the information system; other		
Interview: Organizational personnel with information	ation system security planning and plan implementation responsibilities.(Optional)			
PL-2(CMS-1) – Enhancement (Low)				
Control				
Document the in-place security controls of the sy	stem according to the CMS System Security Plan (SSP) Procedures.			
Applicability: All	References: ARS: PL-2(CMS-1); FISCAM: TSP-2.1; HIPAA: 164.316(b)(1)(i), 164.316(b)(1)(ii); HSPD 7: J(35); IRS-1075: 4.7.3#2	Related Controls:		
ASSESSMENT PROCEDURE: PL-2(CMS-1).1				
Assessment Objective				
Determine if:				
(i) the organization develops and implements a s	security plan for the information system;			
(ii) the security plan provides an overview of the	security requirements for the information system and a description of the security controls planned or in	place for meeting the security requirements;		
(iii) the security plan is consistent with NIST SP	800-18;			
(iv) the security plan is consistent with the organ	ization's information system architecture and information security architecture; and			
(v) designated organizational officials review and approve the security plan.				
Assessment Methods And Objects				
	addressing information system security plan development and implementation; NIST SP 800-18; security			
	in-place security controls of the system are documented according to the CMS System Security Plan (SS			
Interview: Organizational personnel with inform	ation system security planning and plan implementation responsibilities to determine if System Security F	Plan (SSP) includes the in-place security		
	ording to the CMS System Security Plan (SSP) Procedures.			
PL-3 – System Security Plan Update (Lo	ow)	_		
Control				
The SSP shall be reviewed at least every 365 days and updated minimally every three (3) years to reflect current conditions or whenever there are significant changes made to the information system, facilities, or other conditions that may impact security; when the data sensitivity level increases; after a serious security violation; due to changes in the threat environment; or before the previous accreditation expires.				
Guidance				
Significant changes are defined in advance by the organization and identified in the configuration management process. NIST SP 800-18 provides guidance on security plan updates.				
Applicability: All	References: ARS: PL-3; FISCAM: TSP-2.2; HIPAA: 164.306(a)(3), 164.316(a), 164.316(b)(2)(iii); HSPD 7: G(24), J(35); IRS-1075: 5.6.1.2#1.4; NIST 800-53/53A: PL-3; PISP: 4.12.3	Related Controls:		

ASSESSMENT PROCEDURE: PL-3.1

Assessment Objective

Determine if:

(i) the organization defines the frequency of information system security plan reviews and updates;

(ii) the organization updates the security plan in accordance with organization-defined frequency, at least annually;

(iii) the organization receives input to update the security plan from the organization's configuration management and control process; and

(iv) the updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing information system security plan updates; information system security plan; configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records.

PL-4 – Rules of Behavior (ROB) (Low)

Control

ROBs shall be established, and made readily available, to delineate clearly user responsibilities and expected behavior of all Business Owners, users, operators, and administrators with regard to information and information system usage. Before authorizing access to the information system and / or information and annually thereafter, the organization shall receive a signed acknowledgement from all users indicating that they have read, understand, and agree to abide by the ROBs. Specific ROBs shall be established to govern work-at-home users who access CMS information or information systems.

Limited personal use of organization-owned or leased equipment and resources shall be considered to be a permitted use of organization-owned or leased equipment and resources when the following conditions are met:

4.12.4.1. Such use involves minimal additional expense to CMS;

4.12.4.2. Such use does not interfere with the mission or operation of CMS;

4.12.4.3. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch;

4.12.4.4. Such use does not overburden any CMS information system resources;

4.12.4.5. Such use is not otherwise prohibited under this policy; and

4.12.4.6. Any use of organizational Internet and email resources shall be made with the understanding that such use is not secure, private or anonymous.

The following uses of organization-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited:

4.12.4.7. Activities that are in violation of law, Government-wide rule or regulation or that are otherwise inappropriate for the workplace;

4.12.4.8. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-on identification and passwords;

4.12.4.9. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity;

4.12.4.10. All email communications to groups of employees that are subject to approval prior to distribution and have not been approved by the organization (e.g., retirement announcements, union notices or announcements, charitable solicitations); and

4.12.4.11. Employees shall not use the Internet for any purpose, which would reflect negatively on CMS or its employees.

All employees shall have a reasonable expectation of privacy in the workplace. However, employee users of organization-owned or leased equipment and resources shall not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in this policy. To the extent that employees desire to protect their privacy, employees shall not use organization-owned or leased equipment and resources.

Guidance

Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST SP 800-18 provides guidance on preparing rules of behavior.

Applicability: All	References: ARS: PL-4; FISCAM: TSP-3.3.2; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075:	Related Controls:
	5.6.1.2#1.5; NIST 800-53/53A: PL-4; PISP: 4.12.4	

ASSESSMENT PROCEDURE: PL-4.1

Assessment Objective

Determine if:

(i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage;

(ii) the organization makes the rules available to all information system users;

(iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and

(iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Assessment Methods And Objects Examine: Security planning policy; procedures addressing rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records. Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior.(Optional) PL-4(CMS-1) – Enhancement (Low) Control Define user roles and expectations for system and network use. Applicability: All References: ARS: PL-4(CMS-1) **Related Controls:** ASSESSMENT PROCEDURE: PL-4(CMS-1).1 Assessment Objective Determine if: (i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage: (ii) the organization makes the rules available to all information system users: (iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and (iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information. **Assessment Methods And Objects** Examine: Security planning policy; procedures for the development and implementation of rules of behavior for information system users; NIST SP 800-18; rules of behavior; other relevant documents or records to determine user roles and expectations for system and network use are defined. Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior to determine user roles and expectations for system and network use are defined. PL-4(CMS-2) – Enhancement (Low) Control Electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). Applicability: All References: ARS: PL-4(CMS-2) **Related Controls:** ASSESSMENT PROCEDURE: PL-4(CMS-2).1 **Assessment Objective** Determine if: (i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage; (ii) the organization makes the rules available to all information system users; (iii) the rules of behavior for organizational personnel are consistent with NIST SP 800-18; and (iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information. **Assessment Methods And Objects** Examine: Security planning policy: procedures for the development and implementation of rules of behavior for information system users: NIST SP 800-18: rules of behavior; other relevant documents or records to determine electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior to determine electronic signatures are acceptable as signed acknowledgement of rules-of-behavior (ROB). PL-5 – Privacy Impact Assessment (PIA) (Low) Control PIAs shall be conducted for CMS information systems. The PIAs shall be compliant with the E-Government Act of 2002, OMB Memorandum M-03-22, and the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations. Guidance OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002. Applicability: All: Optional for ABMAC, COB, CWF. References: ARS: PL-5: HSPD 7: J(35): NIST 800-53/53A: PL-5: PISP: 4.12.5 **Related Controls:** DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS. ZPIC

ASSESSMENT PROCEDURE: F	՚L-5.1		
Assessment Objective			
Determine if:			
() 0	privacy impact assessment on the information system in accordance with OMB policy; and		
	ent is consistent with federal legislation and OMB policy.		
Assessment Methods And Obj			
Examine: Security planning pol relevant documents or records.	icy; procedures addressing privacy impact assessments on the information system; appropriate f	federal legislation and OMB policy; privacy impact assessment; other	
PL-6 – Security-Related Act	ivity Planning (Low)		
Control			
Security-related activities affecti	ng the information system shall be planned and coordinated before being performed in order to r	reduce the impact on CMS operations (i.e., mission, functions, image,	
and reputation), organizational a	assets, and individuals. Routine security-related activities include, but are not limited to, security	assessments, audits, system hardware and software maintenance,	
security certifications, and testin	g / exercises. Organizational advance planning and coordination includes both emergency and	non-emergency (i.e., routine) situations.	
Guidance			
Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.			
Applicability: All	References: ARS: PL-6; NIST 800-53/53A: PL-6; PISP: 4.12.6	Related Controls:	
ASSESSMENT PROCEDURE: F	²L-6.1		
Assessment Objective			
Determine if:			
(i) the organization plans and co	pordinates security-related activities affecting the information system before conducting such acti	ivities in order to reduce the impact on organizational operations,	
organizational assets, and indiv	iduals; and		
(ii) the organization's advance p	lanning and coordination of security-related activities includes both emergency and non-emergen	ncy situations.	
Assessment Methods And Obj	ects		
Examine: Security planning pol	icy: procedures addressing security-related activity planning for the information system; other rel	lovant documents or records (Ontional)	

Examine: Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records.(Optional)

Interview: Organizational personnel with information system security planning and plan implementation responsibilities.(Optional)

Personnel Security (PS) - Operational

PS-1 – Personnel Security Policy and	Procedures (Low)	
Control		
CMS information systems shall employ perso	nnel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations, s	standards, and guidelines. Procedures shall b
developed to guide the implementation of per		
Guidance		
	are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and gu	uidance. The personnel security policy can be
	curity policy for the organization. Personnel security procedures can be developed for the security progra	
system, when required. NIST SP 800-12 prov	ides guidance on security policies and procedures.	
Applicability: All	References: ARS: PS-1; FISCAM: TSD-1.3.3; IRS-1075: 5.6.2.1#1.1-2; NIST 800-53/53A: PS-1; PISP: 4.13.1	Related Controls:
ASSESSMENT PROCEDURE: PS-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and documents		
	ecurity policy and procedures to appropriate elements within the organization;	
	periodically review personnel security policy and procedures; and	
	ty policy and procedures when organizational review indicates updates are required.	
Assessment Methods And Objects		
Examine: Personnel security policy and proce		
Interview: Organizational personnel with pers	connel security responsibilities (Ontional)	
	solution accounty responsibilities. (Optional)	
ASSESSMENT PROCEDURE: PS-1.2	onner seeung responsibilities. (Optional)	
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if:		
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er	
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures addres	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures addres Assessment Methods And Objects	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures address Assessment Methods And Objects Examine: Personnel security policy and proce	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementati edures; other relevant documents or records.	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures addres Assessment Methods And Objects Examine: Personnel security policy and procedure Interview: Organizational personnel with personnel with personnel security policy and procedures and personnel with	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementati edures; other relevant documents or records.	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures address Assessment Methods And Objects Examine: Personnel security policy and proce	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementati edures; other relevant documents or records.	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures addres Assessment Methods And Objects Examine: Personnel security policy and procedures Interview: Organizational personnel with personnel with personnel security policy and procedures and personnel with	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementati edures; other relevant documents or records.	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures address Assessment Methods And Objects Examine: Personnel security policy and procedure Interview: Organizational personnel with personnel with personnel security policy and procedure of the personnel security policy and personnel secu	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementati edures; other relevant documents or records.	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures addres Assessment Methods And Objects Examine: Personnel security policy and proce Interview: Organizational personnel with personnel PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures addres Assessment Methods And Objects Examine: Personnel security policy and proce Interview: Organizational personnel with personnel PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security procedures addres Assessment Methods And Objects Examine: Personnel security policy and proce Interview: Organizational personnel with personnel PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security policy is consistent (iii) the personnel security policy address Assessment Methods And Objects Examine: Personnel security policy and proce Interview: Organizational personnel with personnel PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1). Assessment Objective	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security policy is consistent (iii) the personnel security policy address Assessment Methods And Objects Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1). Assessment Objective Determine if the organization monitors staff periodical security policy and processes Determine if the organization monitors staff periodical security policy and periodical security periodical security policy and periodical security periodical security periodical security policy and periodical security perio	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security policy is consistent (iii) the personnel security policy address Assessment Methods And Objects Examine: Personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1). Assessment Objective Determine if the organization monitors staff periodical security policy and processes Determine if the organization monitors staff periodical security policy and periodical security periodical security policy and periodical security periodical security periodical security policy and periodical security perio	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security policy is consistent (iii) the personnel security policy and proce Interview: Organizational personnel with personnel security policy and proce Interview: Organizational personnel with personnel PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1). Assessment Objective Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures.	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls. Related Controls: arried out.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security policy is consistent (iii) the personnel security policy and proce Assessment Methods And Objects Examine: Personnel security policy and proce Interview: Organizational personnel with personnel PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1). Assessment Objective Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures.	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls. Related Controls: arried out.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security policy is consistent (iii) the personnel security policy and proce Interview: Organizational personnel with personnel security policy and proce Interview: Organizational personnel with personnel security policy and proce Interview: Organizational personnel with person PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1). Assessment Objective Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions requir	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls. Related Controls: arried out.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security policy is consistent (iii) the personnel security policy and proce Interview: Organizational personnel with personnel security policy and proce Interview: Organizational personnel with personnel PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All ASSESSMENT PROCEDURE: PS-1(FIS-1). Assessment Objective Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions requir Interview: Management and subordinate personnel Staffise Personnel security policy and personnel Staffise performance is monitored on a periodic Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions required Interview: Management and subordinate personnel Determine if the organization monitors staff performance is and procedures. Examine: Select documents or actions required Interview: Management and subordinate personnel Assessment Methods Part Part Part Part Part Part Part Part	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls. Related Controls: arried out.
ASSESSMENT PROCEDURE: PS-1.2 Assessment Objective Determine if: (i) the personnel security policy addresses pu (ii) the personnel security policy is consistent (iii) the personnel security policy is consistent (iii) the personnel security policy and proce Interview: Organizational personnel with personnel with personnel security policy and proce PS-1(FIS-1) – Enhancement (Low) Control Staff's performance is monitored on a periodic Applicability: All Assessment Dejective Determine if the organization monitors staff per Assessment Methods And Objects Examine: Pertinent policies and procedures. Examine: Select documents or actions require Interview: Management and subordinate person PS-1(FIS-2) – Enhancement (Low) Control	rpose, scope, roles and responsibilities, management commitment, coordination among organizational er with the organization's mission and functions and with applicable laws, directives, policies, regulations, st s all areas identified in the personnel security policy and address achieving policy-compliant implementat edures; other relevant documents or records. sonnel security responsibilities.(Optional)	andards, and guidance; and ions of all associated security controls. Related Controls: :arried out. ions, software changes).

ASSESSMENT PROCEDURE: PS-1(FIS-2).1

Assessment Objective

Determine if the organization regularly schedules vacations exceeding several days, where the individual's work is temporarily reassigned, and periodic job/shift rotations are required.

Assessment Methods And Objects

Examine: Personnel records to identify individuals who have not taken vacation or sick leave in the past year.

Examine: Staff assignment records and determine whether job and shift rotations occur.

Examine: Vacation and job rotation policies and procedures.

Interview: Information system management and users.

PS-1(FIS-3) – Enhancement (Low)

Control

Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes. Employees are made aware of their job descriptions.

Applicability: All	References: FISCAM: TSD-1.2.2, TSD-1.3.1, TSP-4.2.1, TSS-2.1.2, TSS-2.1.3	Related Controls:

ASSESSMENT PROCEDURE: PS-1(FIS-3).1

Assessment Objective

Determine if:

(i) the organizational documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and are used for hiring, promoting, and performance evaluation purposes.

(ii) the organization makes the employees aware of their job descriptions.

Assessment Methods And Objects

Examine: Effective dates of the position descriptions and determine whether they are current.

Examine: Job descriptions for several positions in organizational units and for user security administrators.

Examine: Job descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.

Interview: Management personnel.

PS-2 – Position Categorization (Low)

Control

A criticality / sensitivity rating (e.g., non-sensitive, national security, public trust) shall be assigned to all positions within the organization. The criticality / sensitivity rating shall be in compliance with 5 CFR 731.106(a), Executive Orders 10450 and 12968, NSPD-1, HSPD-7, and HSPD-12 and consistent with OPM policy and guidance. Screening criteria shall be established based on the information system access given to the individuals filling those positions. All positions shall be reviewed periodically for criticality / sensitivity rating. All criticality / sensitivity ratings must be submitted to the DHHS HR department and CMS' personnel security department.

Guidance

Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Applicability: All	References: ARS: PS-2; IRS-1075: 5.6.2.1#1.3; NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:

ASSESSMENT PROCEDURE: PS-2.1

Assessment Objective

Determine if:

(i) the organization assigns a risk designations to all positions within the organization;

(ii) the organization establishes a screening criteria for individuals filling organizational positions;

(iii) the risk designations for the organizational positions are consistent with applicable federal regulations and OPM policy and guidance;

(iv) the organization defines the frequency of risk designation reviews and updates for organizational positions; and

(v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan; records of risk designation reviews and updates; other relevant documents or records.

PS-2(0) – Enhancement (Low)

Control

Review and revise position risk designations every 365 days.

Applicability: All	References: ARS: PS-2(0); NIST 800-53/53A: PS-2; PISP: 4.13.2	Related Controls:
ASSESSMENT PROCEDURE: PS-2(0).1		
o 1	ments as specified in the baseline control and the specific CMS requirements as prescribed i	in this amplifying enhancement to the baseline control.
Assessment Methods And Objects		
	s addressing position categorization; appropriate codes of federal regulations; OPM policy ar organization-defined frequency for review of position categorizations); records of risk designation organization-defined frequency for review of position categorizations); records of risk designation of the second	
PS-3 – Personnel Screening (Low)		
Control		
	nd contractors who require access to CMS information or information systems shall be screer prospective employees, references background checks shall be performed before issuance of ith mission critical information.	
Guidance		
	; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational po ablished for the risk designation of the assigned position.	olicy, regulations, and guidance; (iv) FIPS 201 and SP 80
Applicability: All	References: ARS: PS-3; FISCAM: TSP-4.1.1, TSP-4.1.2; IRS-1075: 5.6.2.1#1.4; NIST 80 PS-3; PISP: 4.13.3	00-53/53A: Related Controls:
ASSESSMENT PROCEDURE: PS-3.1		
 (ii) the personnel screening is consistent with an risk designation for the assigned position. Assessment Methods And Objects 	g access to organizational information and information systems prior to authorizing access; an ppropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73 s addressing personnel screening; records of screened personnel; FIPS 201; NIST SP 800-7 rior to employment.	3, 800-76, and 800-78, and the criteria established for the
Applicability: All	References: ARS: PS-3(0); FISCAM: TSP-4.1.2; NIST 800-53/53A: PS-3; PISP: 4.13.3	Related Controls:
ASSESSMENT PROCEDURE: PS-3(0).1		
Assessment Methods And Objects	ments as specified in the baseline control and the specific CMS requirements as prescribed i s for personnel screening; records of screened personnel; FIPS 201; NIST SP 800-73, 800-7	
	security clearance as defined in DHHS Personnel Security/Suitability Handbook.	
Applicability: All ASSESSMENT PROCEDURE: PS-3(CMS-1).	References: ARS: PS-3(CMS-1); FISCAM: TSP-4.1.2	Related Controls:
Assessment Objective Determine if:		
	g access to organizational information and information systems prior to authorizing access; and ppropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST SP 800-73	

Assessment Methods And Objects

Examine: Personnel security policy; procedures for personnel screening; records of screened personnel; and other relevant documents or records to determine that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

Interview: Personnel with personnel screening responsibilities to confirm that all personnel are required to obtain and hold a high-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

PS-4 – Personnel Termination (Low)

Control

Termination procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information and information systems is removed upon personnel termination. Termination procedures shall address:

4.13.4.1. Exit interviews;

4.13.4.2. Retrieval of all organizational information system-related property;

4.13.4.3. Notification to security management;

4.13.4.4. Revocation of all system access privileges;

4.13.4.5. Immediately escorting employees terminated for cause out of organization facilities; and

4.13.4.6. Hard disk back up and sanitization before re-issuance.

Appropriate personnel shall have access to official records created by the terminated employee that are stored on organizational information systems.

Guidance

Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Applicability: All	References: ARS: PS-4; FISCAM: TAC-2.1.6, TSP-4.1.6; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075:	Related Controls:
	5.6.2.1#1.5; NIST 800-53/53A: PS-4; PISP: 4.13.4	

ASSESSMENT PROCEDURE: PS-4.1

Assessment Objective

Determine if:

(i) the organization terminates information system access upon termination of individual employment;

(ii) the organization conducts exit interviews of terminated personnel;

(iii) the organization retrieves all organizational information system-related property from terminated personnel; and

(iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records. **Interview:** Organizational personnel with personnel security responsibilities.(Optional)

PS-4(CMS-1) – Enhancement (Low)

Control

Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination.

Applicability: All	References: ARS: PS-4(CMS-1); FISCAM: TAC-3.2.C.4	Related Controls:
ASSESSMENT PROCEDURE: PS-4(CMS-1).1		

Assessment Objective

Determine if the organization terminates information system access upon termination of individual employment.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records to determine employee access rights are revoked immediately following employee termination, and system access must be revoked prior to or during the employee termination process. **Interview:** Personnel with termination responsibilities to determine employee access rights are revoked immediately following employee to or during the revoked prior to or during

during the employee termination process.

PS-5 – Personnel Transfer (Low)

Control

Transfer procedures shall be developed, documented, and implemented effectively to ensure that access to CMS information or information systems no longer required in the new assignment is terminated upon personnel transfer. Transfer procedures shall address:

4.13.5.1. Re-issuing appropriate organizational information system-related property (e.g., keys, identification cards, building passes); 4.13.5.2. Notification to security management; 4.13.5.3. Closing obsolete accounts and establishing new accounts; and 4.13.5.4. Revocation of all system access privileges (if applicable). Guidance Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts. References: ARS: PS-5; FISCAM: TAC-2.1.6, TSP-4.1.6; IRS-1075; 5.6.2.1#1.6; NIST 800-53/53A: Applicability: All **Related Controls:** PS-5; PISP: 4.13.5 **ASSESSMENT PROCEDURE: PS-5.1 Assessment Objective** Determine if: (i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and (ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization. Assessment Methods And Objects Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records. PS-6 – Access Agreements (Low) Control Individuals who require access to CMS information or information systems shall be required to complete and sign appropriate access agreements, including, but not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements. Guidance Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy. References: ARS: PS-6; FISCAM; TSP-4.1.3; IRS-1075; 5.6.2, 1#1.7; NIST 800-53/53A; PS-6; PISP; Applicability: All **Related Controls:** 4.13.6 ASSESSMENT PROCEDURE: PS-6.1 **Assessment Objective** Determine if: (i) the organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access; (ii) organizational personnel sign access agreements: (iii) the organization defines the frequency of reviews and updates for access agreements; and (iv) the organization reviews and updates the access agreements in accordance with the organization-defined frequency. Assessment Methods And Objects Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records. PS-6(0) – Enhancement (Low) Control Access agreements are reviewed and updated as part of the system accreditation or when a contract is renewed or extended. References: ARS: PS-6(0); NIST 800-53/53A: PS-6; PISP: 4.13.6 Applicability: All **Related Controls:** ASSESSMENT PROCEDURE: PS-6(0).1 **Assessment Objective** Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control. **Assessment Methods And Objects** Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan (for organization-defined frequency for access agreement reviews); access agreements; records of access agreement reviews and updates; other relevant documents or records. Rev. 9 Page 93 of 127 BPSSM Appendix A, Attachment 3

	and Socurity (Low)		
PS-7 – Third-Party Person	iner Security (Low)		
Control	maleured by external earlies providers and third parties shall be desymparted, careed to implem	anted offectively and manit	and for compliance and shall include
	mployed by external service providers and third parties shall be documented, agreed to, implementes, background checks, required expertise, defined security roles and responsibilities, and con		
	all be compliant with CMS IS policies and procedures, and consistent with NIST SP 800-35.	identiality agreements. Te	rsonner security controls employed by service
Guidance			
Third-party providers include,	, for example, service bureaus, contractors, and other organizations providing information system	development, information	technology services, outsourced applications,
and network and security mar	nagement. The organization explicitly includes personnel security requirements in acquisition-rela	ated documents. NIST SP 8	300-35 provides guidance on information
technology security services.			
Applicability: All	References: ARS: PS-7; IRS-1075: 5.6.2.1#1.8; NIST 800-53/53A: PS-7; P	ISP: 4.13.7	Related Controls:
ASSESSMENT PROCEDURE	:: PS-7.1		
Assessment Objective			
Determine if:			
	es personnel security requirements, including security roles and responsibilities, for third-party pro		us, contractors, and other organizations
, °	development, information technology services, outsourced applications, network and security main abult of a service service and the service se	o	
() 0 1)	includes personnel security requirements in acquisition-related documents in accordance with NI third-party provider compliance with personnel security requirements.	ST SP 800-35; and	
Assessment Methods And O			
	policy; procedures addressing third-party personnel security; list of personnel security requirement	ante: acquisition documents	compliance monitoring process: other
relevant documents or record			, compliance monitoring process, other
	rsonnel with personnel security responsibilities; third-party providers.(Optional)		
PS-7(CMS-1) – Enhancement			
Control			
	d to contractors and define security requirements for contractors. Contractors must be provided	with minimal system and ph	vsical access, and must agree to and support
	requirements. The contractor selection process must assess the contractor's ability to adhere to		
Applicability: All			
	References: ARS: PS-7(CMS-1)	••	Related Controls:
ASSESSMENT PROCEDURE			Related Controls:
ASSESSMENT PROCEDURE			Related Controls:
· · · · · · · · · · · · · · · · · · ·			Related Controls:
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe	E: PS-7(CMS-1).1		
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security ma		
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro development, information technology services, outsourced applications, network and security ma third-party provider compliance with personnel security requirements.		
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors Assessment Methods And O	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro development, information technology services, outsourced applications, network and security ma third-party provider compliance with personnel security requirements. Dejects	anagement); and	us, contractors, and other organizations
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors Assessment Methods And O Examine: Personnel security	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathird-party provider compliance with personnel security requirements. Pbjects policy; procedures addressing third-party personnel security; list of personnel security requirement	anagement); and ents; acquisition documents	us, contractors, and other organizations
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors Assessment Methods And O Examine: Personnel security relevant documents or record	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Pbjects policy; procedures addressing third-party personnel security; list of personnel security requirements for contractors and defining security requirements for contractors and security requirements for contractors and security security requirements for contractors and security securit	anagement); and ents; acquisition documents tors. Contractors must be p	us, contractors, and other organizations ; compliance monitoring process; other provided with minimal system and physical
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Pbjects policy; procedures addressing third-party personnel security; list of personnel security requirements for contractors and defining security requirements for contractors and support the CMS information security requirements. The contractor selection process must as	anagement); and ents; acquisition documents tors. Contractors must be p	us, contractors, and other organizations ; compliance monitoring process; other provided with minimal system and physical
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors in Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Pbjects r policy; procedures addressing third-party personnel security; list of personnel security requirements for contractors and defining security requirements for contractor d support the CMS information security requirements. The contractor selection process must as rds.	anagement); and ents; acquisition documents tors. Contractors must be p ssess the contractor's ability	us, contractors, and other organizations c; compliance monitoring process; other provided with minimal system and physical c to adhere to and support CMS' information
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors if Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with thin	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Pbjects policy; procedures addressing third-party personnel security; list of personnel security requirements for contractors and defining security requirements for contractors and support the CMS information security requirements. The contractor selection process must as	anagement); and ents; acquisition documents tors. Contractors must be p ssess the contractor's ability within the security requiren	us, contractors, and other organizations c; compliance monitoring process; other provided with minimal system and physical to adhere to and support CMS' information ments for contractors. Contractors must be
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors if Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with this provided with minimal system	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathin- third-party provider compliance with personnel security requirements. Objects y policy; procedures addressing third-party personnel security; list of personnel security requirements is to determine the access provided to contractors and defining security requirements for contrac- nd support the CMS information security requirements. The contractor selection process must as rds. rd party security responsibilities to determine that the access provided to contractors are defined	anagement); and ents; acquisition documents tors. Contractors must be p ssess the contractor's ability within the security requiren	us, contractors, and other organizations c; compliance monitoring process; other provided with minimal system and physical to adhere to and support CMS' information ments for contractors. Contractors must be
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors if Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with this provided with minimal system	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Objects y policy; procedures addressing third-party personnel security; list of personnel security requirements for contract as to determine the access provided to contractors and defining security requirements for contract as upport the CMS information security requirements. The contractor selection process must as rds. rd party security responsibilities to determine that the access provided to contractors are defined and physical access, and must agree to and support the CMS information security requirements S' information security policies, and standards.	anagement); and ents; acquisition documents tors. Contractors must be p ssess the contractor's ability within the security requiren	us, contractors, and other organizations c; compliance monitoring process; other provided with minimal system and physical to adhere to and support CMS' information ments for contractors. Contractors must be
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors if Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with this provided with minimal system to adhere to and support CMS	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Objects y policy; procedures addressing third-party personnel security; list of personnel security requirements for contract as to determine the access provided to contractors and defining security requirements for contract as upport the CMS information security requirements. The contractor selection process must as rds. rd party security responsibilities to determine that the access provided to contractors are defined and physical access, and must agree to and support the CMS information security requirements S' information security policies, and standards.	anagement); and ents; acquisition documents tors. Contractors must be p ssess the contractor's ability within the security requiren	us, contractors, and other organizations c; compliance monitoring process; other provided with minimal system and physical to adhere to and support CMS' information ments for contractors. Contractors must be
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors i Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with this provided with minimal system to adhere to and support CMS PS-8 – Personnel Sanctio Control The organization shall enforced	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Pbjects r policy; procedures addressing third-party personnel security; list of personnel security requirements for contract ds to determine the access provided to contractors and defining security requirements for contract nd support the CMS information security requirements. The contractor selection process must as rds. rd party security responsibilities to determine that the access provided to contractors are defined n and physical access, and must agree to and support the CMS information security requirements S' information security policies, and standards. ns (Low) e formal personnel sanctions process for personnel who fail to comply with established CMS IS p	anagement); and ents; acquisition documents tors. Contractors must be p seess the contractor's ability within the security requiren s. The contractor selection	us, contractors, and other organizations ; compliance monitoring process; other provided with minimal system and physical r to adhere to and support CMS' information ments for contractors. Contractors must be process must assess the contractor's ability
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors i Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with this provided with minimal system to adhere to and support CMS PS-8 – Personnel Sanctio Control The organization shall enforce consistent with applicable law	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security matchird-party provider compliance with personnel security requirements. Pbjects r policy; procedures addressing third-party personnel security; list of personnel security requirements for contract ds to determine the access provided to contractors and defining security requirements for contract nd support the CMS information security requirements. The contractor selection process must as rds. rd party security responsibilities to determine that the access provided to contractors are defined n and physical access, and must agree to and support the CMS information security requirements S' information security policies, and standards. ns (Low)	anagement); and ents; acquisition documents tors. Contractors must be p seess the contractor's ability within the security requiren s. The contractor selection	us, contractors, and other organizations ; compliance monitoring process; other provided with minimal system and physical r to adhere to and support CMS' information ments for contractors. Contractors must be process must assess the contractor's ability
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors f Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with this provided with minimal system to adhere to and support CMS PS-8 – Personnel Sanction Control The organization shall enforce consistent with applicable law Guidance	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security matchird-party provider compliance with personnel security requirements. Pbjects r policy; procedures addressing third-party personnel security; list of personnel security requirements for contract ds to determine the access provided to contractors and defining security requirements for contract nd support the CMS information security requirements. The contractor selection process must as rds. rd party security responsibilities to determine that the access provided to contractors are defined n and physical access, and must agree to and support the CMS information security requirements S' information security policies, and standards. ns (Low) e formal personnel sanctions process for personnel who fail to comply with established CMS IS p ws, Executive Orders, policies, directives, regulations, standards, and guidelines.	anagement); and ents; acquisition documents tors. Contractors must be p seess the contractor's ability within the security requiren s. The contractor selection policies and procedures. Th	us, contractors, and other organizations ; compliance monitoring process; other provided with minimal system and physical r to adhere to and support CMS' information ments for contractors. Contractors must be process must assess the contractor's ability me employee sanction process shall be
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors the Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with this provided with minimal system to adhere to and support CMS PS-8 – Personnel Sanction Control The organization shall enforce consistent with applicable law Guidance	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Pbjects r policy; procedures addressing third-party personnel security; list of personnel security requirements for contract ds to determine the access provided to contractors and defining security requirements for contract nd support the CMS information security requirements. The contractor selection process must as rds. rd party security responsibilities to determine that the access provided to contractors are defined n and physical access, and must agree to and support the CMS information security requirements S' information security policies, and standards. ns (Low) er formal personnel sanctions process for personnel who fail to comply with established CMS IS pro- vs, Executive Orders, policies, directives, regulations, standards, and guidelines. sistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.	anagement); and ents; acquisition documents tors. Contractors must be p seess the contractor's ability within the security requiren s. The contractor selection policies and procedures. Th	us, contractors, and other organizations ; compliance monitoring process; other provided with minimal system and physical r to adhere to and support CMS' information ments for contractors. Contractors must be process must assess the contractor's ability me employee sanction process shall be
ASSESSMENT PROCEDURE Assessment Objective Determine if: (i) the organization establishe providing information system (ii) the organization monitors if Assessment Methods And O Examine: Personnel security relevant documents or record access, and must agree to an security policies, and standard Interview: Personnel with this provided with minimal system to adhere to and support CMS PS-8 – Personnel Sanction Control The organization shall enforce consistent with applicable law Guidance The sanctions process is consistent	E: PS-7(CMS-1).1 es personnel security requirements, including security roles and responsibilities, for third-party pro- development, information technology services, outsourced applications, network and security mathind-party provider compliance with personnel security requirements. Pbjects r policy; procedures addressing third-party personnel security; list of personnel security requirements for contract ds to determine the access provided to contractors and defining security requirements for contract nd support the CMS information security requirements. The contractor selection process must as rds. rd party security responsibilities to determine that the access provided to contractors are defined n and physical access, and must agree to and support the CMS information security requirements S' information security policies, and standards. ns (Low) er formal personnel sanctions process for personnel who fail to comply with established CMS IS pro- vs, Executive Orders, policies, directives, regulations, standards, and guidelines. sistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.	anagement); and ents; acquisition documents tors. Contractors must be p seess the contractor's ability within the security requiren s. The contractor selection policies and procedures. The uidance. The sanctions proc	us, contractors, and other organizations ; compliance monitoring process; other provided with minimal system and physical r to adhere to and support CMS' information ments for contractors. Contractors must be process must assess the contractor's ability

ASSESSMENT PROCEDURE: PS-8.1			
Assessment Objective			
Determine if:			
	s for personnel failing to comply with established information		
	applicable laws, Executive Orders, directives, policies, regula	ations, standards, and guidance.	
Assessment Methods And Objects			
	ssing personnel sanctions; rules of behavior; records of form		r records.
PS-CMS-1 – Review System Access during E	xtraordinary Personnel Circumstances (Low	v)	
Control			
	nall be reviewed during extraordinary personnel circumstanc	es and limited as deemed necessary.	
Guidance			
A death in the family or other personal problems could to management must consider the circumstances on a case	be considered extraordinary personal circumstances. For so se by case basis.	ome personnel, recovery from a difficult tir	ne may take longer than usual and
	rences: ARS: PS-9; PISP: 4.13.9	R	elated Controls:
ASSESSMENT PROCEDURE: PS-CMS-1.1			
as deemed necessary. Interview: Organizational personnel with personnel sec necessary. PS-CMS-2 – Designate an Information System Control An Information System Security Officer (ISSO) / System Guidance A good reference set for defining the Information System	ther relevant documents or records determine system acces curity responsibilities to determine system access during ext	traordinary personnel circumstances is rev Officer (SSO) (Low) ess component with roles and responsibilit	viewed and access is limited as deemed
protect CMS information systems and data. Applicability: All Refer	rences: ARS: PS-10; FISCAM: TSP-3.1.1, TSP-3.1.2; HIPA	A: 164 308(a)(2): PISP: 4 13 10	elated Controls:
ASSESSMENT PROCEDURE: PS-CMS-2.1			
Assessment Objective			
Determine if the organization has documented the roles	s and responsibilities of appointed ISSO / SSO.		
Assessment Methods And Objects			
Examine: Personnel security policy and procedures; ot	ther relevant documents or records to determine an ISSO / 9	SSO is designated for each component wi	th roles and responsibilities of the position
clearly defined.			

Risk Assessment (RA) - Management

RA-1 – Risk Assessment Policy and Procedures (Low)

Control

All CMS applications and systems shall be covered by an IS RA. The RA shall be consistent with NIST SP 800-30. Formal documented procedures shall be developed, disseminated, and reviewed / updated periodically to facilitate the implementation of the RA policy and associated RA controls. The procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to, current CMS Procedures.

Guidance

The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-30 provides guidance on the assessment of risk. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: RA-1; FISCAM: TAC-3.1.A.2; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075:	Related Controls:
	5.6.1.1#1.1-2; NIST 800-53/53A: RA-1; PISP: 4.14.1	

ASSESSMENT PROCEDURE: RA-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents risk assessment policy and procedures;

(ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization;

- (iii) responsible parties within the organization periodically review risk assessment policy and procedures; and
- (iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.(Optional)

ASSESSMENT PROCEDURE: RA-1.2

Assessment Objective

Determine if:

(i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.(Optional)

RA-2 – Security Categorization (Low)

Control

CMS information systems and the information processed, stored, or transmitted by the systems shall be categorized in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, including, but not limited to the, CMS System Security Level by Information Type. The security categorization (including supporting rationale) shall be explicitly documented. Designated senior-level officials within CMS shall review and approve the security categorizations. CMS shall conduct security categorizations as an organization-wide activity with the involvement of the CMS CIO, CISO, and Business Owners.

All CMS information systems categorized as high or moderate shall be considered sensitive or to contain sensitive information. All CMS information systems categorized as low shall be considered non-sensitive or to contain non-sensitive information. All CMS information systems shall implement minimum security requirements and controls as established in the current CMS IS Standards, based on security categorization of the system.

Guidance

The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST SP 800-60 provides guidance on determining the security categories of the

Applicability: All		References: ARS: RA-2; FISCAM: TAC-1.1; HSPD 7: D(8); IRS-1075: 4.1#2; NIST 800-53/53A: RA-2; PISP: 4.14.2	Related Controls: MP-4, SC-7
ASSESSMENT PROCEDURE: R	RA-2.1		
Assessment Objective			
Determine if:			
		zation of the information system as an organization-wide exercise with the involvement of senior-level	officials including, but not limited to,
(ii) the security categorization is c		chief information officer, senior agency information security officer, and mission/information owners;	
		gorization of the information system, potential impacts to other organizations and, in accordance with t	he LISA PATRIOT Act of 2001 and Homelan
Security Presidential Directives, p			
(iv) the organization includes sup	pporting rationale	for impact-level decisions as part of the security categorization; and	
		s review and approve the security categorization of the information system.	
Assessment Methods And Obje			
		Idressing security categorization of organizational information and information systems; security planni	ng policy and procedures; FIPS 199; NIST S
800-60; information system secur		categorization and risk assessment responsibilities.(Optional)	
RA-3 – Risk Assessment (RA			
	A) (LOW)		
Control			i e di i e di di di di
		t could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of	
		e performed, both within CMS and by external parties that manage / operate information or information	
		d on the operation of the information system, the RA shall take into account vulnerabilities, threat source	es, and security controls in place to determine
the resulting level of residual fisk		perations, CMS assets, CMS information, or individuals.	
Any findings from reviews of CMS	AS systems shall b	be evaluated as to the impact of the vulnerability on the information system. Any identified weaknesses	s shall be documented by the Business Own
		risk, accepting the risk with explanation or submitting Corrective Action Plan (CAP). These findings sh	
established by applicable laws, E	Executive Orders,	directives, policies, regulations, standards, and guidance.	
Guidance			
		s, threat sources, and security controls planned or in place to determine the resulting level of residual r	
		operation of the information system. The organization also considers potential impacts to other organi	
		Il Directives, potential national-level impacts in categorizing the information system. Risk assessments	
		or individuals from external parties (e.g., service providers, contractors operating information systems or tsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication	
		ect nonpublic or privacy-related information. As such, organizational assessments of risk also address	
		Is supporting that portion of the risk assessment dealing with public access to federal information syste	
	cluding threat, vul	nerability, and impact assessments.	1 5
Applicability: All		References: ARS: RA-3; FISCAM: TAC-3.1.A.2, TSP-1.1.2, TSP-1.1.3, TSP-5.1.4; HIPAA:	Related Controls:
		164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075:	
		5.6.1.1#1.3, 6.3.3#2; NIST 800-53/53A: RA-3; PISP: 4.14.3	
ASSESSMENT PROCEDURE: R	RA-3.1		
Assessment Objective			
Determine if:	a rial and magnitu	de of herm that could reput from the upput herized papers, upp displayure disruption modification or	destruction of information and information
		Ide of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or cluding information and information systems managed/operated by external parties); and	
(ii) the risk assessment is consist			
Assessment Methods And Obje			
		ing policy and procedures: procedures addressing organizational assessments of risk: risk assessmen	

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST SP 800-30; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.(Optional)

RA-3(CMS-1) – Enhancement (Low)				
Control Perform an IS RA for the system, and document Investment Framework [FRAMEWORK]).	the risk and safeguards of the system in accordance with the CMS Information Security Risk Assessme	nt (RA) Procedures (See CMS Integrated IT		
Applicability: All	References: ARS: RA-3(CMS-1); FISCAM: TAC-1.1, TAC-1.2, TSS-2.2.4; HIPAA: 164.306(a)(2); HSPD 7: D(8)	Related Controls:		
ASSESSMENT PROCEDURE: RA-3(CMS-1).1				
Assessment Objective				
Determine if the organization assesses the risk a	and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modif and assets (including information and information systems managed/operated by external parties).	ication, or destruction of information and		
Assessment Methods And Objects				
organization-defined frequency for risk assessme	ning policy and procedures; procedures addressing organizational assessments of risk; risk assessment ent updates); records of risk assessment updates; NIST SP 800-30; other relevant documents or record m, and documents the risks and safeguards of the system in accordance with the CMS Information Sec MEWORK]).	s to determine that prior to project initiation,		
safeguards of the system in accordance with the	sessment responsibilities to determine that prior to project initiation, the organization performs an IS RA CMS Information Security Risk Assessment (RA) Procedures (See CMS Integrated IT Investment Framework (RA) Procedures (See CMS Integrated IT Investment Framework)	for the system, and documents the risks and nework [FRAMEWORK]).		
RA-4 – Risk Assessment Update (Low)				
Control				
The RA shall be performed and documented ever status of the system. Further, the requirements	ery three (3) years or whenever there are significant changes to the system, facilities, or other conditions for re-assessments are listed in section 4.4.6, Security Accreditation.	that may impact the security or accreditation		
Guidance				
updates.	fic criteria for what is considered significant change to the information system. NIST SP 800-30 provides			
Applicability: All	References: ARS: RA-4; FISCAM: TAC-1.2, TSD-2.2.2, TSP-1.1; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 5.6.1.1#1.4; NIST 800-53/53A: RA-4; PISP: 4.14.4	Related Controls:		
ASSESSMENT PROCEDURE: RA-4.1				
system resides, or other conditions that may imp	t in accordance with the organization-defined frequency or whenever there are significant changes to the act the security or accreditation status of the system;	information system, the facilities where the		
(iii) the risk assessment update is consistent with				
Assessment Methods And Objects	ded changes based on the organization's experiences during security plan implementation.			
	ning policy and procedures; procedures addressing risk assessment updates; risk assessment; informat	ion system security plan; records of risk		
RA-5 – Vulnerability Scanning (Low)				
Control				
Appropriate vulnerability assessment tools and techniques shall be implemented by the organization. Selected personnel shall be trained in their use and maintenance. The organization shall conduct periodic testing of its security posture by scanning its information systems with vulnerability tools. The information obtained from the vulnerability scanning process shall be shared with appropriate personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems. The activities of employees using organization Internet and email resources shall be subject to monitoring by system or security personnel without notice.				
Guidance				
techniques. Vulnerability scans are scheduled ar	priate scanning tools and techniques. The organization trains selected personnel in the use and mainten nd/or random in accordance with organizational policy and assessment of risk. The information obtained			
	out the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability a ches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source co			

Applicability: All	References: ARS: RA-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); NIST 800-53/53A: RA-5;	Related Controls:
ASSESSMENT PROCEDURE: RA-5.1	PISP: 4.14.5	
Assessment Objective		
Determine if:		
	Inerability scans within the information system;	
and reported;	the information system in accordance with the organization-defined frequency or when significant new vu	
vulnerability management process by using st procedures, and (c) measuring vulnerability im		among tools and automate parts of the aking transparent checklists and test
	bility scanning in accordance with NIST SP 800-42; and	
	ability management in accordance with NIST SP 800-40.	
Assessment Methods And Objects		
management records; other relevant documer	s addressing vulnerability scanning; risk assessment; information system security plan; vulnerability scan	ning results; patch and vulnerability
	assessment and vulnerability scanning responsibilities.(Optional)	
RA-5(CMS-1) – Enhancement (Low)		
Control		
	and conduct enterprise security posture review as needed but no less than once a year, in accordance wit	th CMS IS procedures. Document findings and
	es to Common Vulnerabilities and Exposures (CVE) naming convention.	in cline to procedures. Document indings and
Applicability: All	References: ARS: RA-5(CMS-1); HIPAA: 164.306(a)(2); HSPD 7: G(24)	Related Controls:
ASSESSMENT PROCEDURE: RA-5(CMS-1)).1	-
Assessment Objective		
Determine if:		
	Inerability scans within the information system;	
and reported; and	the information system in accordance with the organization-defined frequency or when significant new vu	
	g tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability andards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and ma spact.	
Assessment Methods And Objects		
vulnerability scanning results; patch and vulne	s addressing vulnerability scanning; risk assessment; information system security plan (for organization-d prability management records; other relevant documents or records to determine the organization perform than once a year. Findings are documented and assessment results and vulnerabilities correlate to Corr	s penetration testing and conducts enterprise
	assessment and vulnerability scanning responsibilities to determine the organization performs penetration ce a year. Findings are documented and assessment results and vulnerabilities correlate to Common Vu	
		, , , ,

System and Services Acquisition (SA) – Management

SA-1 – System and Services Acquisition	Policy and Procedures (Low)			
Control				
	Documented procedures shall be developed and implemented effectively to facilitate the implementation of the system and services acquisition security controls in all system and services acquisitions. Procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.			
Guidance				
The system and services acquisition policy and	procedures are consistent with applicable laws, Executive Orders, directives,	policies, regulations, standards, and guidance. The system and services		
acquisition policy can be included as part of the general, and for a particular information system.	general information security policy for the organization. System and services when required. NIST SP 800-12 provides guidance on security policies and p	icquisition procedures can be developed for the security program in rocedures.		
Applicability: All	References: ARS: SA-1; IRS-1075: 5.6.1.3#1.1-2; NIST 800-53/53A: SA-1;			
ASSESSMENT PROCEDURE: SA-1.1	· · · · · · · · · · · · · · · · · · ·			
Assessment Objective				
Determine if:				
(i) the organization develops and documents sys	stem and services acquisition policy and procedures;			
(ii) the organization disseminates system and se	rvices acquisition policy and procedures to appropriate elements within the or	ganization;		
	eriodically review system and services acquisition policy and procedures; and			
(iv) the organization updates system and service	es acquisition policy and procedures when organizational review indicates upo	ates are required.		
Assessment Methods And Objects				
	y and procedures; other relevant documents or records.			
· · · · · · · · · · · · · · · · · · ·	n and services acquisition responsibilities.(Optional)			
ASSESSMENT PROCEDURE: SA-1.2				
Assessment Objective				
Determine if:				
	dresses purpose, scope, roles and responsibilities, management commitment			
	consistent with the organization's mission and functions and with applicable la			
	res address all areas identified in the system and services acquisition policy a	nd address achieving policy-compliant implementations of all associated		
security controls.				
Assessment Methods And Objects				
	y and procedures; other relevant documents or records.			
	n and services acquisition responsibilities.(Optional)			
SA-2 – Allocation of Resources (Low)				
Control				
	ontrol processes, CMS or the external organization shall determine, document			
	ncluded in mission / business case planning, and a separate line item shall be	established in CMS' programming and budgeting documentation for the		
implementation and management of information	systems security.			
Guidance		ning and antablish as a discuste line item for information systems are with		
I ne organization includes the determination of s	ecurity requirements for the information system in mission/business case plar g documentation. NIST SP 800-65 provides guidance on integrating security i	ning and establishes a discrete line item for information system security		
Applicability: All	References: ARS: SA-2: NIST 800-53/53A: SA-2: PISP: 4.15.2	Related Controls:		
ASSESSMENT PROCEDURE: SA-2.1	References. And: OA 2, NICT 000 30,00A. OA 2, 1101 . 4.13.2	Related Controls.		
Assessment Objective				
Determine if:				
(i) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system;				
(ii) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system, (ii) the organization determines security requirements for the information system in mission/business case planning;				
(iii) the organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation; and				
(iv) the organization's programming and budgeti				
	.			

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST SP 800-65; other relevant documents or records. Interview: Organizational personnel with capital planning and investment responsibilities.(Optional)

SA-3 – Life Cycle Support (Low)

Control

A uniform System Development Life-Cycle (SDLC) methodology shall be established and followed to manage all CMS information systems.

Guidance

NIST SP 800-64 provides guidance on security considerations in the system development life cycle. References: ARS: SA-3; FISCAM: TAY-1.2.1, TCC-1.1.2; NIST 800-53/53A: SA-3; PISP: 4.15.3

Applicability: All

ASSESSMENT PROCEDURE: SA-3.1

Assessment Objective

Determine if:

(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and

(ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation; other relevant documents or records.

Interview: Organizational personnel with information security and system life cycle development responsibilities.(Optional)

SA-3(CMS-1) - Enhancement (Low)

Control

Must comply with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

Applicability: All	References: ARS: SA-3(CMS-1); FISCAM: TCC-1.1.1	Related Controls:		
ASSESSMENT PROCEDURE: SA-3(CMS-1).1				

Assessment Objective

Determine if:

(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and

(ii) the organization uses a system development life cycle that is consistent with NIST SP 800-64.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST SP 800-64; information system development life cycle documentation: other relevant documents or records to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

Interview: Organizational personnel with information security and system life cycle development responsibilities to determine the organization complies with the information security steps of IEEE 12207.0 standard for SDLC, as defined by CMS and/or the CMS FRAMEWORK.

SA-3(FIS-1) – Enhancement (Low)

Control

Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.

Applicability: All	References: FISCAM: TCC-2.1.2	Related Controls:

ASSESSMENT PROCEDURE: SA-3(FIS-1).1

Assessment Objective

Determine if the organizational detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.

Assessment Methods And Objects

Examine: Design system specifications.

Examine: Pertinent policies and procedures.

Interview: Programmer and programming supervisor.

Related Controls:

SA-4 – Acquisitions (Low)		
Control	instigned shall be included, either explicitly or by reference, in all information system apo	nuisition contracts based on an approximent of risk in apportance
with applicable laws, Executive Orders, direct	ications shall be included, either explicitly or by reference, in all information system acc ctives, policies, regulations, and standards.	quisition contracts based on an assessment of risk in accordance
Solicitation Documents Solicitation documents (e.g., Request for Pro 4.15.4.1. Security capabilities; 4.15.4.2. Design and development processe 4.15.4.3. Test and evaluation procedures; ar 4.15.4.4. Documentation.		security requirements that describe the required:
The requirements in the solicitation documer	nts shall permit updating security controls as new threats / vulnerabilities are identified	and as new technologies are implemented
Use of Evaluated and Validated Products		
For acquisition of security and security-enab	led commercial-off-the-shelf (COTS) information technology products, when multiple p lated through one or more of the following sources:	roducts meet CMS requirements, preference shall be given to
 The National Information Assurance Partn The International Common Criteria Recog The NIST Cryptographic Module Validatio 		
Configuration Settings and Implementation C The information system required documenta	Guidance tion shall include security configuration settings, including documentation explaining ex	cceptions to the standard, and security implementation guidance.
Guidance		
capabilities (security needs and, as necessa procedures; and (iv) required documentation	or Proposals) for information systems and services include, either explicitly or by refere ry, specific security controls and other specific FISMA requirements); (ii) required desig I. The requirements in the solicitation documents permit updating security controls as n dance on the selection of information security products. NIST SP 800-35 provides guida s in the system development life cycle.	gn and development processes; (iii) required test and evaluation new threats/vulnerabilities are identified and as new technologies are
Information System Documentation		
The solicitation documents include requirement	ents for appropriate information system documentation. The documentation addresses controls in the information system. The level of detail required in the documentation is	
Use of Tested, Evaluated, and Validated Pro NIST SP 800-23 provides guidance on the a	oducts cquisition and use of tested/evaluated information technology products.	
	Suidance tion includes security configuration settings and security implementation guidance. OM s. NIST SP 800-70 provides guidance on configuration settings for information technolo	
Applicability: All	References: ARS: SA-4; NIST 800-53/53A: SA-4; PISP: 4.15.4	Related Controls:
ASSESSMENT PROCEDURE: SA-4.1		
Assessment Objective		
Determine if:		
accordance with applicable laws, Executive	nents and/or security specifications, either explicitly or by reference, in information sys Orders, directives, policies, regulations, and standards; cial information technology products is consistent with NIST SP 800-23;	tem acquisition contracts based on an assessment of risk and in
	rgs and security implementation guidance in organizational acquisitions are consistent	with NIST SP 800-70; and
Rev. 9	Page 102 of 127	BPSSM Appendix A, Attachment

(iv) acquisition contracts for	information systems include	either explicitly or by reference	e. security requirements and	l/or security specifications that describe:
(1) acquisition contracto ion			s, cocamy requiremente and	a crocond operation and december

- required security capabilities;
- required design and development processes;
- required test and evaluation procedures; and
- required documentation.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.(Optional)

SA-4(CMS-1) – Enhancement (Low)

Control

Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

Applicability: All	References: ARS: SA-4(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SA-4(CMS-1) 1		

Assessment Objective

Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST SP 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records to determine that all contracts and Statements of Work (SOW) that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities to determine that all contracts and SOW that require development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities and receive approval from CMS officials.

SA-5 – Information System Documentation (Low)

Control

Procedures shall be developed, documented, and implemented effectively to ensure that adequate documentation for all CMS information systems and its constituent components is available, protected when required, and distributed only to authorized personnel. The administrative and user guides and/or manuals shall include information on configuring, installing, and operating the information system, and for optimizing the system's security features. The guides and/or manuals shall be reviewed periodically, and, if necessary, updated as new vulnerabilities are identified and/or new security controls are added.

Guidance

Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Applicability: All	References: ARS: SA-5; FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1, TSD-3.1.2, TSD-3.1.3, TSP- 3.3.2; IRS-1075: 5.6.1.3#1.3; NIST 800-53/53A: SA-5; PISP: 4.15.5	Related Controls:
ACCESSMENT DROOFDURE: OA 54		

ASSESSMENT PROCEDURE: SA-5.1 Assessment Objective

Determine if:

(i) the organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system;

(ii) the organization makes available information on configuring, installing, and operating the information system; and

(iii) the organization makes available information on effectively using the security features in the information system.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; other relevant documents or records.

Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system. (Optional)

SA-5(CMS-1) – Enhancement (Low)		
Control		
	specify the purpose, technical operation, access, maintenance, and	required training for administrators and users.
	ARS: SA-5(CMS-1); FISCAM: TSD-1.1.6, TSD-3.1.1	Related Controls:
ASSESSMENT PROCEDURE: SA-5(CMS-1).1		
Assessment Objective		
Determine if the organization includes, in addition to administra	ator and user guides, documentation, if available from the vendor/ma sufficient detail to permit analysis and testing of the controls (includir	anufacturer, describing the design and implementation details of the ng functional interfaces among control components).
Assessment Methods And Objects		
guides; other relevant documents or records to determine the o maintenance; and required personnel training to include admini	organization develops system documentation to describe the system istrators and users.	
	ocumentation responsibilities; organizational personnel operating, u ystem's purpose; description; technical operations and access; mair	
SA-5(CMS-2) – Enhancement (Low)		
Control		
Maintain an updated list of related system operations and secu	rity documentation.	
Applicability: All References:	ARS: SA-5(CMS-2); FISCAM: TSD-1.1.6	Related Controls:
ASSESSMENT PROCEDURE: SA-5(CMS-2).1		
Assessment Methods And Objects Examine: System and services acquisition policy; procedures a guides; other relevant documents or records to determine the o	organization maintains an updated list of related system's operations ocumentation responsibilities; organizational personnel operating, u	; information system documentation including administrator and user s and security documentation.
SA-5(CMS-3) – Enhancement (Low)		
Control Update documentation upon changes in system functions and p security of hard copies depending on data sensitivity included in	processes. Must include date and version number on all formal sys n the documentation.	tem documentation. Refer to "Media Protection" standard for
	ARS: SA-5(CMS-3); FISCAM: TCC-2.1.10, TSD-1.1.6, TSD-3.1.1	Related Controls:
ASSESSMENT PROCEDURE: SA-5(CMS-3).1		
Assessment Methods And Objects Examine: System and services acquisition policy; procedures a		; information system documentation including administrator and user
formal system documentation. Refer to "Media Protection" star Interview: Organizational personnel with information system do	organization updates documentation upon changes in system function and for security of hard copies depending on data sensitivity include ocumentation responsibilities; organizational personnel operating, up functions and processes. Must include date and version number on rity included in the documentation.	ded in the documentation. Ising, and/or maintaining the information system to determine if the
SA-5(FIS-1) – Enhancement (Low)		
Control Goals are established by senior management on the availability with the goals and surveys user departments to see if their nee	y of data processing and on-line services. Senior management peri ds are being met.	iodically reviews and compares the service performance achieved
Rev. 9	Page 104 of 127	BPSSM Appendix A, Attachment 3

Applicability: All	References: FISCAM: TSC-2.4.6, TSC-2.4.9	Related Controls:
ASSESSMENT PROCEDURE: SA-5(FIS-1).1		
Assessment Objective		
	shed by senior management on the availability of data processing and on-line services. Senior managen	nent periodically reviews and compares the
	d surveys user departments to see if their needs are being met.	
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation.		
Interview: Senior management, data processing SA-5(FIS-2) – Enhancement (Low)	g management, and user management.	
Control	an fa an a fan an fan ach ad dae . Dachte an an didelana an an dae	
identify recurring patterns or trends.	ice in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time t	or resolution are recorded and analyzed to
Applicability: All	References: FISCAM: TSC-2.4.7, TSC-2.4.8	Related Controls:
ASSESSMENT PROCEDURE: SA-5(FIS-2).1		Trefated Controls.
Assessment Objective		
	tained on the actual performance in meeting service schedules. Problems and delays encountered, the	reason and the elapsed time for resolution are
recorded and analyzed to identify recurring patter		sacon, and the slapsed time for recolution are
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Supporting documentation.		
Interview: Senior management, data processing	g management, and user management.	
SA-6 – Software Usage Restrictions (Lo	ow)	
Control		
All software or shareware and associated docum	nentation used on CMS information systems shall be deployed and maintained in accordance with appro	priate license agreements and copyright laws.
	y quantity licenses shall be managed through a tracking system to control copying and distribution. All o	
5	of publicly accessible peer-to-peer file sharing technology shall be controlled and documented to ensure	that this capability is not used for the
unauthorized distribution, display, performance,		
Guidance	d in accordance with contract agreements and copyright laws. For software and associated documentati	ion protocted by quantity licenses, the
	I copying and distribution. The organization controls and documents the use of publicly accessible peer-	
	stribution, display, performance, or reproduction of copyrighted work.	to peer me sharing teermology to ensure that
Applicability: All	References: ARS: SA-6; FISCAM: TCC-2.3.1; IRS-1075: 4.7.3#1.2; NIST 800-53/53A: SA-6; PISP:	Related Controls:
	4.15.6	
ASSESSMENT PROCEDURE: SA-6.1		
Assessment Objective		
Determine if:		
(i) the organization complies with software usage		
	oftware usage for indications of inappropriate or unusual activity, investigates suspicious activity or susp	ected violations, reports findings to
appropriate officials, and takes necessary action Assessment Methods And Objects	S.	
-	y; procedures addressing software usage restrictions; site license documentation; list of software usage	restrictions: other relevant decuments or
records.	y, procedures addressing sortware usage restrictions, site incense documentation, list of sortware usage	
	ation system administration responsibilities; organizational personnel operating, using, and/or maintainin	g the information system.(Optional)
SA-6(FIS-1) – Enhancement (Low)		
Control		
	are provided to all locations where they are maintained on file.	
	•	

Applicability: All	F	References: FISCAM: TCC-2.3.2		Related Controls:
ASSESSMENT PROCEDU				
Assessment Objective	· ·			
Determine if the organizat	ation provides to all locatio	ons software implementation orders, including effective da	te, where the orders are maintained on	ı file.
Assessment Methods And	nd Objects			
Examine: Implementatior	on orders.			
Examine: Pertinent polici	cies and procedures.			
Interview: Information system		strators.		
SA-7 – User Installed S	Software (Low)			
Control				
		stalling software, unless explicitly authorized in writing by		tative. Users that have been granted such
Guidance	oad and install only organi	ization-approved software. The use of install-on-demand	software shall be restricted.	
	v privileges users have the	e ability to install software. The organization identifies wh	at types of software installations are per	mitted (e.g. undates and security natches to
		re prohibited (e.g., software that is free only for personal,		
malicious is unknown or s			not government doe, and certifate inte	e poligiou mariogara lo sonig polonially
Applicability: All	F	References: ARS: SA-7; FISCAM: TCC-1.3.1; NIST 800-	53/53A: SA-7; PISP: 4.15.7	Related Controls:
ASSESSMENT PROCEDU	URE: SA-7.1			
Assessment Objective				
Determine if:				
(i) the organization enforc	ces explicit rules governin	g the installation of software by users;		
(ii) unauthorized software	e is present on the system	; and		
	, ,	er installed software for indications of inappropriate or unit	usual activity, investigates suspicious act	ivity or suspected violations, reports findings to
appropriate officials, and	2			
Assessment Methods And	-			
Examine: System and se relevant documents or red		procedures addressing user installed software; list of rule	s governing user installed software; netv	vork traffic on the information system; other
		on system administration responsibilities; organizational		aining the information system.(Optional)
		are on the information system; information system for pro	nibited software.(Optional)	
SA-7(CMS-1) – Enhancem	nent (Low)			
Control				
If user installed software i	is authorized in writing by	the CIO or his/her designated representative, ensure that	t business rules and technical controls e	nforce the documented authorizations and
prohibitions.				
Applicability: All		References: ARS: SA-7(CMS-1)		Related Controls:
ASSESSMENT PROCEDU	URE: SA-7(CMS-1).1			
Assessment Objective				
Determine if the organizat	ation enforces explicit rules	s governing the installation of software by users.		
Assessment Methods And	nd Objects			
relevant documents or rec	ecords to determine that po	procedures addressing user installed software; list of rule olicies exist that ensure business rules and technical cont	rols enforce the documented authorization	ons and prohibitions.
		on system administration responsibilities; organizational ical controls enforce the documented authorizations and		aining the information system to determine that
SA-9 – External Information	nation System Servi	ces (Low)		
Control				
		de specific provisions requiring the service provider to co		
compliance. CMS shall d	define the remedies for an	y loss, disruption, or damage caused by the service provi vriting, by the CMS CIO or his/her designated representation	der's failure to comply. Service provider	s shall be prohibited from outsourcing any system

Guidance

An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. NIST SP 800-35 provides guidance on the security considerations in the system development life cycle.

		References: ARS: SA-9; FISCAM: TAY-1.3.1; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4; NIST 800-53/53A: SA-9; PISP: 4.15.9	Related Controls: CA-3
--	--	--	------------------------

ASSESSMENT PROCEDURE: SA-9.1

Assessment Objective

Determine if:

(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;

(ii) the organization monitors security control compliance;

(iii) the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions; and

(iv) the security controls employed by providers of external information system services are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.(Optional)

SA-9(CMS-1) – Enhancement (Low)

Control

If service providers are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas, ensure that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Applicability: All	References: ARS: SA-9(CMS-1); HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8)	Related Controls:
ASSESSMENT PROCEDURE: SA-9(CMS-1).1		

Assessment Objective

Determine if the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services to determine that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance for service providers who are authorized in writing by the CMS CIO or his/her designated representative to outsource any system function overseas.

System and Communications Protection (SC) – *Technical*

SC-1 – System and Communications Protection Policy and Procedures (Low)

Control

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

Guidance

The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Applicability: All	References: ARS: SC-1; FISCAM: TAC-3.2.E.1; IRS-1075: 5.6.3.4#1, 5.6.3.4#2; NIST 800-53/53A: SC-1; PISP: 4.16.1	Related Controls:

ASSESSMENT PROCEDURE: SC-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents system and communications protection policy and procedures;

(ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and

(iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and communications protection responsibilities.(Optional)

ASSESSMENT PROCEDURE: SC-1.2

Assessment Objective

Determine if:

(i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and

(iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with system and communications protection responsibilities.(Optional)

SC-2 – Application Partitioning (Low)

Control

User interface services (e.g., web services) shall be separated physically or logically from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Guidance

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Applicability: All	References: ARS: SC-2; NIST 800-53/53A: SC-2; PISP: 4.16.2	Related Controls:
ASSESSMENT PROCEDURE: SC-2.1		

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Test: Separation of user functionality from information system management functionality.(Optional)

SC-2(CMS-1) - Enhancement (Low)

Control

Implement DMZ architecture to separate internal network from public systems, and CMS servers from unnecessary public access, physically partitioning applications of varying sensitivity levels.

Applicability: All	References: ARS: SC-2(CMS-1)	Related Controls:

ASSESSMENT PROCEDURE: SC-2(CMS-1).1

Assessment Objective

Determine if the information system separates user functionality (including user interface services) from information system management functionality.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

Interview: Selected organizational personnel with network administration responsibilities to determine if the organization places all CMS servers allowing public access within a DMZ environment, and disallows direct access to the internal network. DMZ servers can only access the internal network by utilizing DMZ packet filtering and proxy rules to provide protection for CMS servers.

SC-5 – Denial of Service Protection (Low)

Control

Mechanisms shall be established to prevent, or limit the effects of well-known, detectable, and preventable denial-of-service attacks.

Guidance

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Applicability: All	References: ARS: SC-5; NIST 800-53/53A: SC-5; PISP: 4.16.5	Related Controls:
ASSESSMENT PROCEDURE: SC-5.1		

Assessment Objective

Determine if:

(i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and

(ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records.

Test: Information system for protection against or limitation of the effects of denial of service attacks.(Optional)

SC-5(0) – Enhancement (Low)

Control

Protect the information system against the denial-of-service attacks defined on the following sites or within the following documents:

- SANS Organization www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and
- NIST CVE List http://checklists.nist.gov/home.cfm.

		References: ARS: SC-5(0); NIST 800-53/53A: SC-5; PISP: 4.16.5	Related Controls.	
1	Applicability: All	References: ARS: SC-5(0): NIST 800-53/53A: SC-5: PISP: 4.16.5	Related Controls:	

ASSESSMENT PROCEDURE: SC-5(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan (for list of organization-defined types of denial of service attacks to protect against or limit); information system configuration settings and associated documentation; other relevant documents or records.

SC-5(1) – Enhancement (Low)				
Control				
	rvice attacks against other information systems or networks.			
Applicability: All	References: ARS: SC-5(1); NIST 800-53/53A: SC-5(1)	Related Controls:		
ASSESSMENT PROCEDURE: SC-5(1).1				
Assessment Objective				
	ability of users to launch denial of service attacks against other information systems or networks.			
Assessment Methods And Objects				
Examine: System and communications protection associated documentation; other relevant docum	on policy; procedures addressing denial of service protection; information system design documentation;	information system configuration settings and		
	or limitation of the effects of denial of service attacks].(Optional)			
SC-5(2) – Enhancement (Low)				
Control				
	dundancy to limit the effects of information flooding types of denial of service attacks.			
Applicability: All	References: ARS: SC-5(2); NIST 800-53/53A: SC-5(2)	Related Controls:		
ASSESSMENT PROCEDURE: SC-5(2).1				
Assessment Objective				
	cess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial	of service attacks.		
Assessment Methods And Objects				
	on policy; procedures addressing denial of service protection; information system design documentation;	information system configuration settings and		
associated documentation; other relevant docum	nents or records].(Optional)			
SC-7 – Boundary Protection (Low)				
Control				
	all be established and supporting procedures shall be developed, documented, and implemented effectiv			
the external boundary of the information system	and at key internal boundaries within the system. Any connections to the Internet, or other external netw illure of the boundary protection mechanisms shall not result in any unauthorized release of information of	Orks or information systems, shall occur		
	designated alternate processing site shall provide the same levels of protection as those of the primary s			
Guidance				
	I networks or information systems, occur through managed interfaces consisting of appropriate boundary	protection devices (e.g., proxies, gateways,		
routers, firewalls, guards, encrypted tunnels) arra	anged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on	a protected subnetwork commonly referred to		
as a demilitarized zone or DMZ). Information sys	stem boundary protections at any designated alternate processing sites provide the same levels of protections	tion as that of the primary site.		
As part of a defense in depth protection strategy	the organization considers partitioning higher impact information systems into congrate physical domain	ns (or onvironments) and applying the		
	As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection			
of appropriate candidates for domain partitioning				
	The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services.			
	mmonly based on network components and consolidated management systems shared by all attached o			
	party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-77 provides guidance on			
virtual private networks.				
Applicability: All	References: ARS: SC-7; NIST 800-53/53A: SC-7; PISP: 4.16.7	Related Controls: AC-4, CA-3, MP-4, RA-2		
		,		
ASSESSMENT PROCEDURE: SC-7.1				
Assessment Objective				
Determine if:				

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records. **Interview:** Selected organizational personnel with boundary protection responsibilities.(Optional)

Test: Information system monitoring and control of communications at the external boundary of the information system and at key internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system. (Optional)

SC-7(5) – Enhancement (Low)

Control

Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required.

Applicability: All	References: ARS: SC-7(5); FISCAM: TAC-3.2.E.1	Related Controls:
ASSESSMENT PROCEDURE: SC-7(5).1		

Assessment Objective

Determine if the information system denies network traffic by default and allows network traffic by exception.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.(Optional)

Interview: Selected organizational personnel with boundary protection responsibilities.(Optional)

SC-7(CMS-1) – Enhancement (Low)

Control

Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Applicability: All	References: ARS: SC-7(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SC-7(CMS-1).1		

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.

SC-7(CMS-2) – Enhancement (Low)

Control

Although not required, it is recommended that stateful inspection hardware and software is utilized.

Applicability: All	References: ARS: SC-7(CMS-2); FISCAM: TAC-3.2.E.1	Related Controls:
ASSESSMENT PROCEDURE: SC-7(CMS-2).1		

Assessment Objective

Determine if:

(i) the organization defines key internal boundaries of the information system; and

(ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records to determine if the organization utilizes stateful inspection / application firewall hardware and software.

Interview: Selected organizational personnel with boundary protection responsibilities to determine if the organization utilizes stateful inspection / application firewall hardware and software.

SC-10 – Network Disconnect (Low)			
Control			
Technical controls shall be established and implemented effectively to ensure that network connections are properly terminated at the end of user sessions, or upon the occurrence of specified conditions (e.g., a period of inactivity).			
Guidance			
The organization applies this control within the co	pontext of risk management that considers specific mission or operational requirements.		
Applicability: All	References: ARS: SC-10; NIST 800-53/53A: SC-10; PISP: 4.16.10	Related Controls:	
ASSESSMENT PROCEDURE: SC-10.1			
Assessment Objective			
Determine if:			
(i) the organization defines the time period of inac	ctivity before the information system terminates a network connection; and		
(ii) the information system terminates a network of	connection at the end of a session or after the organization-defined time period of inactivity.		
Assessment Methods And Objects			
	n policy; procedures addressing network disconnect; information system design documentation; organiz	zation-defined time period of inactivity before	
	ation settings and associated documentation; other relevant documents or records.(Optional)		
Test: Network disconnect capability within the int	formation system.(Optional)		
SC-10(0) – Enhancement (Low)			
Control			
	onnect network connections at the end of a session, or after fifteen (15) minutes of inactivity, for mainfra		
·· · ·	References: ARS: SC-10(0); FISCAM: TAC-3.2.C.3; PISP: 4.16.10	Related Controls:	
ASSESSMENT PROCEDURE: SC-10(0).1			
Assessment Objective			
Determine if the organization meets the requirem	ents as specified in the baseline control and the specific CMS requirements as prescribed in this amplify	ying enhancement to the baseline control.	
Assessment Methods And Objects			
Examine: System and communications protection	n policy; procedures addressing network disconnect; information system design documentation; organiz	ation-defined time period of inactivity before	
network disconnect; information system configura	ation settings and associated documentation; other relevant documents or records.		
SC-13 – Use of Cryptography (Low)			
Control			
	edures shall be developed, documented, and implemented effectively to ensure they comply with applic	able laws, Executive Orders, directives,	
policies, regulations, standards, and guidance. A	Il such mechanisms shall be FIPS 140-2 (as amended and revised) compliant and NIST validated.		
Guidance			
The applicable federal standard for employing cr	yptography in non-national security information systems is FIPS 140-2 (as amended). Validation certification	ates issued by the NIST Cryptographic Module	
	140-2, and future amendments) remain in effect and the modules remain available for continued use an		
specifically revoked. NIST SP 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.			
Applicability: All	References: ARS: SC-13; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2,	Related Controls: AC-17(CMS-1), AC-	
Applicability: All	5.6.3.4#4.2-3; NIST 800-53/53A: SC-13; PISP: 4.16.13	19(CMS-1), AC-3, AC-3(CMS-1), MP-	
		4(PII-1), SC-12(CMS-1), SC-8(CMS-1),	
		SC-9(1)	
ASSESSMENT PROCEDURE: SC-13.1			
Assessment Objective			
	nic protection, the information system implements cryptographic mechanisms that comply with applicable	e laws. Executive Orders, directives, policies.	
regulations, standards, and guidance.			

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST SP 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

SC-14 – Public Access Protectio	ns (Low)	
Control		
Technical controls shall be developed,	documented, and implemented effectively to protect the integrity of the publicly accessible	CMS information and applications.
Guidance		
CMS refers to the National Institute of	Standards and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix A	provides a summary for remote access controls.
Applicability: All	References: ARS: SC-14; NIST 800-53/53A: SC-14; PISP: 4.16.14	Related Controls:
ASSESSMENT PROCEDURE: SC-14	.1	
Assessment Objective		
-	otects the integrity and availability of publicly available information and applications.	
Assessment Methods And Objects		
	s protection policy; procedures addressing public access protections; access control policy	and procedures; boundary protection procedures; information
system design documentation; informa	ation system configuration settings and associated documentation; other relevant documents	s or records.
	enting access controls and boundary protection for publicly available information and applic	ations within the information system.(Optional)
SC-14(CMS-1) – Enhancement (Low)		
Control		
Ensure that network access controls, o	operating system file permissions, and application configurations protect the integrity of infor	rmation stored, processed, and transmitted by publicly accessible
systems, as well as the integrity of pub		
Applicability: All	References: ARS: SC-14(CMS-1); FISCAM: TAC-3.2.E.1	Related Controls:
ASSESSMENT PROCEDURE: SC-14	(CMS-1).1	
Assessment Objective		
, , , ,	otects the integrity and availability of publicly available information and applications.	
Assessment Methods And Objects		
	as protection policy; procedures addressing public access protections; access control policy	
	ation system configuration settings and associated documentation; and other relevant docum	
	on configurations protect the integrity of information stored, processed, and transmitted by pu	ublicly accessible systems, as well as the integrity of publicly
accessible applications.	o determine if network access controls, operating system file permissions, and application co	onfigurations protect the integrity of information stored, processed
and transmitted by publicly accessible	systems, as well as the integrity of publicly accessible applications.	oningurations protect the integrity of information stored, processed,
SC-14(CMS-2) – Enhancement (Low)		
Control		
	lemented in conjunction with an related to public occess protections, refer to APS Annendiv	A for a Authentication Standarda
Applicability: All	lemented in conjunction with or related to public access protections, refer to ARS Appendix / References: ARS: SC-14(CMS-2)	Related Controls:
ASSESSMENT PROCEDURE: SC-14		Related Controls.
	(CIN-5-2). I	
Assessment Objective		
	otects the integrity and availability of publicly available information and applications.	
Assessment Methods And Objects		
	is protection policy; procedures addressing public access protections; access control policy	
	ation system configuration settings and associated documentation; and other relevant docun ated to public access protections, refer to ARS Appendix A for e-Authentication Standards.	nents of records to determine if e-authentication is required and
	-facing MA to determine if e-authentication is required and implemented in conjunction with a	or related to public access protections: refer to ARS Appendix A for
e-Authentication Standards.		
SC-CMS-1 – Desktop Modems (I	() () () () () () () () () () () () () (
Control		
Users are prohibited from installing de	sktop modems	
Guidance		
	a the network putting the CMS date and network at very high risk	
	o the network putting the CMS data and network at very high risk.	
Rev. 9	Page 113 of 127	BPSSM Appendix A, Attachment
		PP

Applicability: All	References: ARS: SC-CMS-1; PISP: 4.16.24	Related Controls:
ASSESSMENT PROCEDURE	:: SC-CMS-1.1	
Assessment Objective		
	has implement a policy which assists in prohibiting the installation of unauthorized desktop modems.	
Assessment Methods And C		
	icy does not allow unauthorized desktop modems.	
SC-CMS-2 – Identify and I	Detect Unauthorized Modems (Low)	
Control		
	ted procedures shall be established, documented and implemented effectively to identify and detect unaut	thorized modems.
Guidance		
	gement approve any automated tool or utility for checking for unauthorized modems.	
Applicability: All	References: ARS: SC-CMS-2; PISP: 4.16.25	Related Controls:
ASSESSMENT PROCEDURE	:: SC-CMS-2.1	
Assessment Objective		
	has an approved automated system to test for unauthorized modems.	
Assessment Methods And O		
Examine: Network documen	tation to determine if network systems use an automated method to determine if unnecessary network ser	vices (e.g., modems, etc.) are available on demand and the
	plete review no less than quarterly. rsonnel to determine if network systems use an automated method to determine if unnecessary network s	arriana (a.a. madama ata) ara available an demand and the
	plete review no less than quarterly.	ervices (e.g., moderns, etc.) are available on demand and the
SC-CMS-2(CMS-0) – Enhanc		
Control		
	k systems using an automated method no less than quarterly to determine if unauthorized modems are pre	asant
Applicability: All	References: ARS: SC-CMS-2(CMS-0)	Related Controls:
ASSESSMENT PROCEDURE		
Assessment Objective		
	meets the requirements as specified in the baseline control and the specific CMS requirements as prescri	ibed in this amplifying enhancement to the baseline control
Assessment Methods And C		
	tation to determine if network systems use an automated method to determine if unnecessary network ser	vices (e.g., modems, etc.) are available on demand and the
	plete review no less than quarterly.	
	isonnel to determine if network systems use an automated method to determine if unnecessary network s	ervices (e.g., modems, etc.) are available on demand and the
Interview: Organizational pe	plete review no less than quarterly.	ervices (e.g., modems, etc.) are available on demand and the
Interview: Organizational pe organization performs a com		ervices (e.g., modems, etc.) are available on demand and the
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A	plete review no less than quarterly.	ervices (e.g., modems, etc.) are available on demand and the
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control	plete review no less than quarterly. uthentication and Encryption (Low)	
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control	plete review no less than quarterly.	
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control Appropriate technical controls network.	plete review no less than quarterly. uthentication and Encryption (Low)	
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control Appropriate technical controls network. Guidance	plete review no less than quarterly. uthentication and Encryption (Low)	
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control Appropriate technical controls network. Guidance A good place to obtain techni	plete review no less than quarterly. uthentication and Encryption (Low) s shall be developed, documented, and implemented effectively to assure the identity of users and protect	
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control Appropriate technical controls network. Guidance A good place to obtain technical Applicability: All	plete review no less than quarterly. Authentication and Encryption (Low) s shall be developed, documented, and implemented effectively to assure the identity of users and protect ical controls for handling sensitive information in-transit is the NIST SP. References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26	the in-transit confidentiality of their sessions outside the secur
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control Appropriate technical controls network. Guidance	plete review no less than quarterly. Authentication and Encryption (Low) s shall be developed, documented, and implemented effectively to assure the identity of users and protect ical controls for handling sensitive information in-transit is the NIST SP. References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26	the in-transit confidentiality of their sessions outside the secur
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control Appropriate technical controls network. Guidance A good place to obtain techni Applicability: All ASSESSMENT PROCEDURE Assessment Objective	plete review no less than quarterly. Authentication and Encryption (Low) s shall be developed, documented, and implemented effectively to assure the identity of users and protect ical controls for handling sensitive information in-transit is the NIST SP. References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26	the in-transit confidentiality of their sessions outside the secu
Interview: Organizational pe organization performs a com SC-CMS-3 – Secondary A Control Appropriate technical controls network. Guidance A good place to obtain techni Applicability: All ASSESSMENT PROCEDURE Assessment Objective	plete review no less than quarterly. Authentication and Encryption (Low) s shall be developed, documented, and implemented effectively to assure the identity of users and protect ical controls for handling sensitive information in-transit is the NIST SP. References: ARS: SC-CMS-3; FISCAM: TAC-3.2.E.1; PISP: 4.16.26 E: SC-CMS-3.1 has policies in place to provide technical controls to protect sensitive data in-transit.	the in-transit confidentiality of their sessions outside the secu

SC-CMS-3(CMS-0) – Enhancement (Low)		
Control		
No specific requirements but recommend enabli	ing application security mechanisms, such as Transport Layer Security (TLS), and utilizing minimum en	cryption and password authentication.
Applicability: All	References: ARS: SC-CMS-3(CMS-0)	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-3(CM	IS-0).1	
Assessment Objective		
Determine if the organization meets the requirer	ments as specified in the baseline control and the specific CMS requirements as prescribed in this ampli	fying enhancement to the baseline control.
Assessment Methods And Objects		
	ganization enables and forces use of application security mechanisms, such as TLS. The organization us on with certificate-based authentication or additional authentication protection (e.g., token-based, biometer and the security of the s	
	ne if the organization enables and forces use of application security mechanisms, such as TLS. The org ination with certificate-based authentication or additional authentication protection (e.g., token-based, bio	
SC-CMS-3(CMS-1) – Enhancement (Low)		
Control		
If e-authentication is required and implemented,	refer to ARS Appendix A for e-Authentication Standards controls and procedures.	
Applicability: All	References: ARS: SC-CMS-3(CMS-1)	Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-3(CM	IS-1).1	
Assessment Objective		
Determine if the organization that uses e-auther	ntication is required to refer to ARS Appendix A for e-Authentication Standards controls and procedures.	
Assessment Methods And Objects		
	which recommends enabling application security mechanisms, such as TLS, and utilizing minimum enc	ryption and password authentication although,
no specific requirements are mandatory.		
	ne if enabling application security mechanisms is recommended, such as TLS, and utilizing minimum en	cryption and password authentication although,
no specific requirements are mandatory.		
SC-CMS-5 – Persistent Cookies (Low)		
Control		
	e is prohibited unless explicitly approved in writing by the DHHS Secretary.	
Guidance		
Requests to DHHS should be via CMS.		
	References: ARS: SC-CMS-5; PISP: 4.16.28	
		Related Controls:
ASSESSMENT PROCEDURE: SC-CMS-5.1		Related Controls:
Assessment Objective		
Assessment Objective Determine if the organization does not use a per	rsistent cookie configuration on a CMS web site to remember subsequent visits unless approved in writi	
Assessment Objective Determine if the organization does not use a per Assessment Methods And Objects		
Assessment Objective Determine if the organization does not use a per Assessment Methods And Objects Examine: CMS web site baseline and change m	nanagement documentation for configurations using persistent cookies.	ng by the DHHS Secretary.
Assessment Objective Determine if the organization does not use a per Assessment Methods And Objects Examine: CMS web site baseline and change m Interview: Web site administrators to determine Secretary.	nanagement documentation for configurations using persistent cookies. If the CMS web site has persistent cookies enable in the baseline configuration or have written approva	ng by the DHHS Secretary.
Assessment Objective Determine if the organization does not use a per Assessment Methods And Objects Examine: CMS web site baseline and change m Interview: Web site administrators to determine	nanagement documentation for configurations using persistent cookies. If the CMS web site has persistent cookies enable in the baseline configuration or have written approva	ng by the DHHS Secretary.
Assessment Objective Determine if the organization does not use a per Assessment Methods And Objects Examine: CMS web site baseline and change m Interview: Web site administrators to determine Secretary.	nanagement documentation for configurations using persistent cookies. If the CMS web site has persistent cookies enable in the baseline configuration or have written approva	ng by the DHHS Secretary.
Assessment Objective Determine if the organization does not use a per Assessment Methods And Objects Examine: CMS web site baseline and change m Interview: Web site administrators to determine Secretary. SC-CMS-6 – Network Interconnection (I Control	nanagement documentation for configurations using persistent cookies. If the CMS web site has persistent cookies enable in the baseline configuration or have written approva	ng by the DHHS Secretary. al to enable persistent cookies from the DHHS
Assessment Objective Determine if the organization does not use a per Assessment Methods And Objects Examine: CMS web site baseline and change m Interview: Web site administrators to determine Secretary. SC-CMS-6 – Network Interconnection (I Control	nanagement documentation for configurations using persistent cookies. If the CMS web site has persistent cookies enable in the baseline configuration or have written approva	ng by the DHHS Secretary. al to enable persistent cookies from the DHHS
Assessment Objective Determine if the organization does not use a per Assessment Methods And Objects Examine: CMS web site baseline and change m Interview: Web site administrators to determine Secretary. SC-CMS-6 – Network Interconnection (I Control Control Controls shall be developed, documented, and i Guidance	nanagement documentation for configurations using persistent cookies. If the CMS web site has persistent cookies enable in the baseline configuration or have written approva	ng by the DHHS Secretary. al to enable persistent cookies from the DHHS

ASSESSMENT PROCEDUR	E: SC-CMS-6.1	
Assessment Objective		
-	n effectively documents and implements authorized network interconnections external to the system boundarie	ies.
Assessment Methods And	Objects	
Examine: Documentation to	o determine remote location(s) follow all CMS IS policies and standards for all external interconnections.	
SC-CMS-6(CMS-0) - Enhan	cement (Low)	
Control		
	e.g., users and sites using a network interconnection external to the system boundaries) follow all CMS IS poli nent the interconnection in the SSP for the system that is connected to the remote location.	icies and standards and obtain a signed Interconnection
Applicability: All	References: ARS: SC-CMS-6(CMS-0); FISCAM: TAC-2.1.3, TAC-2.3.2	Related Controls:
ASSESSMENT PROCEDUR	E: SC-CMS-6(CMS-0).1	
Assessment Objective		
Determine if the organizatio	n meets the requirements as specified in the baseline control and the specific CMS requirements as prescribe	ed in this amplifying enhancement to the baseline control.
Assessment Methods And	Objects	
	o determine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection S onnected to the remote location.	Security Agreement. Document the interconnection in the
Interview: Personnel to det the system that is connected	ermine remote location(s) follow all CMS IS policies and standards and obtain a signed Interconnection Secur d to the remote location.	rity Agreement. Document the interconnection in the SSP for

System and Information Integrity (SI) – Operational

SI-1 – System and Information Integrity Policy and Procedures (I
--

Control

Automated mechanisms for system, software, and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to systems, software, and information. The procedures and automated mechanisms shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Guidance

The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures. It is good practice to have an automated system which is host based to automatically detect, block/filter and alert supervisors or managers that possible unauthorized changes to software and the information system have occurred.

Applicability: All References: ARS: SI-1; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-1; PISP: 4.17.1 Related Controls:	PISP: 4 17 1	
---	--------------	--

ASSESSMENT PROCEDURE: SI-1.1

Assessment Objective

Determine if:

(i) the organization develops and documents system and information integrity policy and procedures;

(ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization;

(iii) responsible parties within the organization periodically review system and information integrity policy and procedures; and

(iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.

Interview: Organizational personnel with system and information integrity responsibilities.(Optional)

ASSESSMENT PROCEDURE: SI-1.2

Assessment Objective

Determine if:

(i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;

(ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records. **Interview:** Organizational personnel with system and information integrity responsibilities.(Optional)

SI-2 – Flaw Remediation (Low)

Control

Information system flaws in an operational CMS information system shall be identified, reported and effective remedial actions shall be taken. Systems affected by recently announced software vulnerabilities shall be identified. Patches, service packs, and hot fixes shall be tested for effectiveness and potential side effects on the CMS information systems prior to installation. The flaw remediation process shall be centrally managed and updates shall be installed automatically without individual user intervention.

Guidance

The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. It is a good practice to test the changes in a laboratory environment on like systems prior to approving and implementing the updates and changes. NIST SP 800-40, provides guidance on security patch installation and patch management.

Applicability: All References: ARS: SI-2; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST & PISP: 4.17.2	800-53/53A: SI-2; Related Controls: CA-2, CA-4, CA-7, CM- 3, IR-4, SI-11
---	---

ASSESSMENT PROCEDURE: SI-2.1

Assessment Objective

Determine if:

(i) the organization identifies, reports, and corrects information system flaws:

(ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures;

(iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures:

(iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and

(v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.(Optional)

SI-2(0) – Enhancement (Low)

Control

Correct identified information system flaws on production equipment within one (1) month.

(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and

(b) Manage the flaw remediation process centrally.

Applicability: All	References: ARS: SI-2(0); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2; NIST 800-53/53A: SI-2;	Related Controls:
	FISF: 4.17.2	

ASSESSMENT PROCEDURE: SI-2(0).1

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; NIST SP 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws: other relevant documents or records.

Interview: Organizational personnel with flaw remediation responsibilities.(Optional)

SI-2(1) – Enhancement (Low)

Control

Updates are installed automatically.

Applicability: All	References: ARS: SI-2(1); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2	Related Controls:
ASSESSMENT PROCEDURE: SI-2(1).1		

Assessment Objective

Determine if the organization centrally manages the flaw remediation process and installs updates automatically.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates: information system design documentation: information system configuration settings and associated documentation: list of information system flaws: list of recent security flaw remediation actions performed on the information system; other relevant documents or records. (Optional)

Test: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates.(Optional)

SI-2(2) – Enhancement (Low) Control Employ automated mechanisms periodically and upon demand to determine the state of information system components with regard to flaw remediation

Employ automated mechanisms periodically and o	apon demand to determine the state of information system components with regard to haw remediation.	
Applicability: All	References: ARS: SI-2(2); HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2	Related Controls:

ASSESSMENT PROCEDURE: SI-2(2).1

Assessment Objective

Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation. Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records.(Optional)

Test: Automated mechanisms implementing information system flaw remediation update status.(Optional)

SI-3 – Malicious Code Protection (Low)

Control

Automated malicious code protection mechanisms that include a capability of automatic updates shall be in place and supporting procedures shall be developed, documented, and implemented effectively to identify and isolate suspected malicious software. Antiviral mechanisms shall be implemented effectively and maintained, at critical information system entry points, and at each workstation, server, or mobile computing device on the network to detect and eradicate malicious code transported by email, email attachments, removable media or other methods. Business owners shall use antiviral software products from multiple vendors, if possible, and update virus protection mechanisms whenever new releases are available.

Guidance

The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and the resulting potential impact on the availability of the information system. NIST SP 800-83 provides guidance on implementing malicious code protection.

Applicability: All	References: ARS: SI-3; FISCAM: TCC-1.3.2; IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP:	Related Controls:
	4.17.3	

ASSESSMENT PROCEDURE: SI-3.1

Assessment Objective

Determine if:

(i) the information system implements malicious code protection;

(ii) the organization employs malicious code protection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code;

(iii) the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities;

(iv) the organization updates malicious code protection mechanisms whenever new releases are available; and

(v) the malicious code protection mechanisms are appropriately updated to include the latest malicious code definitions, configured to perform periodic scans of the information system as well as realtime scans of files from external sources as the files are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(0) – Enhancement (Low)

Control

Implement malicious code protection at information system entry points, including firewalls, email servers, remote access servers, workstations, servers, and mobile computing devices by employing automated mechanisms to detect and eradicate malicious code transported by email, email attachments, and removable media.

Applicability: All	References: ARS: SI-3(0); IRS-1075: 5.6.2.5#1.3; NIST 800-53/53A: SI-3; PISP: 4.17.3	Related Controls:
ASSESSMENT PROCEDURE: SI-3(0).1		

Assessment Objective

Determine if the organization meets the requirements as specified in the baseline control and the specific CMS requirements as prescribed in this amplifying enhancement to the baseline control.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious code protection mechanisms; records of malicious code protection

SI-3(1) – Enhancement (Low)	guration settings and associated documentation; other relevant documents or records.	
Control		
	de protection software centrally with automatic updates for the latest malicious code definition	s whenever new releases are available
Applicability: All	References: ARS: SI-3(1); IRS-1075: 5.6.2.5#1.3	Related Controls:
ASSESSMENT PROCEDURE: SI		
Assessment Objective		
-	trally manages malicious code protection mechanisms.	
Assessment Methods And Obje		
	n integrity policy; procedures addressing malicious code protection; information system design	n documentation; malicious code protection mechanisms; records of
	s; information system configuration settings and associated documentation; other relevant do	
SI-3(2) – Enhancement (Low)		
Control		
	o update malicious code protection.	
Applicability: All	References: ARS: SI-3(2); IRS-1075: 5.6.2.5#1.3	Related Controls:
ASSESSMENT PROCEDURE: SI	-3(2).1	
Assessment Objective		
Determine if the organization auto	matically updates malicious code protection mechanisms.	
Assessment Methods And Obje		
	n integrity policy; procedures addressing malicious code protection; information system desig	
	s; information system configuration settings and associated documentation; other relevant do for malicious code protection.(Optional)	cuments or records.(Optional)
SI-3(CMS-1) – Enhancement (Lo		
	w)	
Control	esktop malicious code scanning software must be installed, real-time protection and monitorir	a must be enabled, and the software must be configured to perform
critical system file scans during s		ig must be enabled, and the software must be configured to perform
Applicability: All	References: ARS: SI-3(CMS-1); IRS-1075: 5.6.2.5#1.3	Related Controls:
ASSESSMENT PROCEDURE: SI		
Assessment Objective		
Determine if:		
(i) real-time file scanning is enable		
	ed;	
	de scanning is enabled and monitored; and	
Assessment Methods And Obje	de scanning is enabled and monitored; and orm critical system file scans during system boot and once a week.	
	de scanning is enabled and monitored; and orm critical system file scans during system boot and once a week. cts	
	de scanning is enabled and monitored; and orm critical system file scans during system boot and once a week. cts n integrity policy; procedures addressing malicious code protection; NIST SP 800-83; maliciou	
week.	de scanning is enabled and monitored; and orm critical system file scans during system boot and once a week. cts n integrity policy; procedures addressing malicious code protection; NIST SP 800-83; maliciou iguration settings and associated documentation; other relevant documents or records to dete	ermine real-time file scanning is enabled. Desktop malicious code
Interview. Personnel with system	de scanning is enabled and monitored; and orm critical system file scans during system boot and once a week. cts n integrity policy; procedures addressing malicious code protection; NIST SP 800-83; maliciou	ermine real-time file scanning is enabled. Desktop malicious code
	de scanning is enabled and monitored; and form critical system file scans during system boot and once a week. cts in integrity policy; procedures addressing malicious code protection; NIST SP 800-83; maliciou iguration settings and associated documentation; other relevant documents or records to dete ed, real-time protection and monitoring must be enabled, and the software must be configured in and information integrity responsibilities to determine real-time file scanning is enabled, des	ermine real-time file scanning is enabled. Desktop malicious code d to perform critical system file scans during system boot and once a ktop malicious code scanning software is installed, real-time protection.
and monitoring is enabled, and th	de scanning is enabled and monitored; and form critical system file scans during system boot and once a week. cts n integrity policy; procedures addressing malicious code protection; NIST SP 800-83; maliciou iguration settings and associated documentation; other relevant documents or records to dete ed, real-time protection and monitoring must be enabled, and the software must be configured and information integrity responsibilities to determine real-time file scanning is enabled, des e software is configured to perform critical system file scans during system boot and once a w	ermine real-time file scanning is enabled. Desktop malicious code d to perform critical system file scans during system boot and once a ktop malicious code scanning software is installed, real-time protection
and monitoring is enabled, and th	de scanning is enabled and monitored; and form critical system file scans during system boot and once a week. cts in integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious iguration settings and associated documentation; other relevant documents or records to dete ed, real-time protection and monitoring must be enabled, and the software must be configured in and information integrity responsibilities to determine real-time file scanning is enabled, des	ermine real-time file scanning is enabled. Desktop malicious code d to perform critical system file scans during system boot and once a ktop malicious code scanning software is installed, real-time protection
and monitoring is enabled, and th	de scanning is enabled and monitored; and form critical system file scans during system boot and once a week. cts n integrity policy; procedures addressing malicious code protection; NIST SP 800-83; maliciou iguration settings and associated documentation; other relevant documents or records to dete ed, real-time protection and monitoring must be enabled, and the software must be configured and information integrity responsibilities to determine real-time file scanning is enabled, des e software is configured to perform critical system file scans during system boot and once a w	ermine real-time file scanning is enabled. Desktop malicious code d to perform critical system file scans during system boot and once a ktop malicious code scanning software is installed, real-time protection
and monitoring is enabled, and th SI-4 – Information System Mo Control	de scanning is enabled and monitored; and form critical system file scans during system boot and once a week. cts n integrity policy; procedures addressing malicious code protection; NIST SP 800-83; maliciou iguration settings and associated documentation; other relevant documents or records to dete ed, real-time protection and monitoring must be enabled, and the software must be configured and information integrity responsibilities to determine real-time file scanning is enabled, des e software is configured to perform critical system file scans during system boot and once a w	ermine real-time file scanning is enabled. Desktop malicious code d to perform critical system file scans during system boot and once a ktop malicious code scanning software is installed, real-time protection, reek.
and monitoring is enabled, and th SI-4 – Information System Mo Control Effective monitoring tools and tec Guidance	de scanning is enabled and monitored; and orm critical system file scans during system boot and once a week. cts n integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious iguration settings and associated documentation; other relevant documents or records to dete ed, real-time protection and monitoring must be enabled, and the software must be configured and information integrity responsibilities to determine real-time file scanning is enabled, des e software is configured to perform critical system file scans during system boot and once a we onitoring Tools and Techniques (Low) hniques providing real-time identification of unauthorized use, misuse, and abuse of the inform	ermine real-time file scanning is enabled. Desktop malicious code d to perform critical system file scans during system boot and once a ktop malicious code scanning software is installed, real-time protection veek.
and monitoring is enabled, and th SI-4 – Information System Mo Control Effective monitoring tools and tec Guidance Information system monitoring ca	de scanning is enabled and monitored; and prim critical system file scans during system boot and once a week. cts in integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious iguration settings and associated documentation; other relevant documents or records to detected, real-time protection and monitoring must be enabled, and the software must be configured in and information integrity responsibilities to determine real-time file scanning is enabled, des e software is configured to perform critical system file scans during system boot and once a vertex onitoring Tools and Techniques (Low) hniques providing real-time identification of unauthorized use, misuse, and abuse of the inform pability is achieved through a variety of tools and techniques (e.g., intrusion detection system	ermine real-time file scanning is enabled. Desktop malicious code d to perform critical system file scans during system boot and once a ktop malicious code scanning software is installed, real-time protection veek. nation system shall be implemented. s, intrusion prevention systems, malicious code protection software,
and monitoring is enabled, and th SI-4 – Information System Mo Control Effective monitoring tools and tec Guidance Information system monitoring ca audit record monitoring software,	de scanning is enabled and monitored; and orm critical system file scans during system boot and once a week. cts n integrity policy; procedures addressing malicious code protection; NIST SP 800-83; malicious iguration settings and associated documentation; other relevant documents or records to dete ed, real-time protection and monitoring must be enabled, and the software must be configured and information integrity responsibilities to determine real-time file scanning is enabled, des e software is configured to perform critical system file scans during system boot and once a we onitoring Tools and Techniques (Low) hniques providing real-time identification of unauthorized use, misuse, and abuse of the inform	ermine real-time file scanning is enabled. Desktop malicious code d to perform critical system file scans during system boot and once a ktop malicious code scanning software is installed, real-time protection reek. mation system shall be implemented. s, intrusion prevention systems, malicious code protection software, ation system (e.g., at selected perimeter locations, near server farms

	urity changes to the information system. The granularity of the information collected is determined by the organization	based upon its monitoring objectives and the
capability of the information system	n to support such activities. Organizations consult appropriate legal counsel with regard to all information system moni ring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or inc	itoring activities. Organizations neighten the
	nng activity whenever there is an indication of increased risk to organizational operations, organizational assets, or inc n, or other credible sources of information. NIST SP 800-61 provides guidance on detecting attacks through various ty	
	alware-based attacks through malicious code protection software. NIST SP 800-92 provides guidance on monitoring a	
	e on intrusion detection and prevention.	ind analyzing computer security event logs.
Applicability: All	References: ARS: SI-4; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800- 53/53A: SI-4; PISP: 4.17.4	Related Controls: AC-8, AU-4, CM-6
ASSESSMENT PROCEDURE: SI-4		
Assessment Objective		
Determine if the organization emplo	oys tools and techniques to monitor events on the information system, detect attacks, and provide identification of una	authorized use of the system.
Assessment Methods And Object	ts	
-	integrity policy; procedures addressing information system monitoring tools and techniques; information system desig	an documentation: information system
monitoring tools and techniques do	ocumentation; information system configuration settings and associated documentation; other relevant documents or r	ecords.(Optional)
SI-4(1) – Enhancement (Low)		
Control		
	a common IDS management network using common protocols.	
Applicability: All	References: ARS: SI-4(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4; NIST 800-53/53A: SI-4(1)	Related Controls:
ASSESSMENT PROCEDURE: SI-4	4(1).1	
Assessment Objective		
Determine if the organization interc	connects and configures individual intrusion detection tools into a systemwide intrusion detection system using commo	on protocols.
Determine if the organization interce Assessment Methods And Object	· · · · ·	on protocols.
Assessment Methods And Object	· · · · ·	
Assessment Methods And Object Examine: System and information monitoring tools and techniques do	ts	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional)	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system desig ocumentation; information system configuration settings and associated documentation; information system protocols;	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intro	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system desig	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intro	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system desig ocumentation; information system configuration settings and associated documentation; information system protocols;	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional)	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system desig ocumentation; information system configuration settings and associated documentation; information system protocols;	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system desig ocumentation; information system configuration settings and associated documentation; information system protocols;	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system desig ocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional)	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of information	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design ocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional)	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informatic) (c) Signaling to an external informatic)	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design ocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional)	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions.	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design ocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or	n documentation; information system other relevant documents or
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design ocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5)	n documentation; information system
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design ocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5)	n documentation; information system other relevant documents or
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design ocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5)	n documentation; information system other relevant documents or
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if:	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design pocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1	n documentation; information system other relevant documents or
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design becomentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 tions of compromise or potential compromise to the security of the information system; and	n documentation; information system other relevant documents or
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica (ii) the information system provides	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design becomentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 Ations of compromise or potential compromise to the security of the information system; and is a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur.	n documentation; information system other relevant documents or
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica (ii) the information system provides Assessment Methods And Object	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design becomentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 tions of compromise or potential compromise to the security of the information system; and s a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ts	n documentation; information system other relevant documents or Related Controls:
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informati (c) Signaling to an external informati (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica (ii) the information system provides Assessment Methods And Object Examine: System and information	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design bocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 tions of compromise or potential compromise to the security of the information system; and is a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ts integrity policy; procedures addressing information system monitoring tools and techniques; information system security integrity policy; procedures addressing information system monitoring tools and techniques; information system security integrity policy; procedures addressing information system monitoring tools and techniques; information system security colls and techniques; information security colls and techniques; information security colls and techniques; information security colls a	n documentation; information system other relevant documents or Related Controls:
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica (ii) the information system provides Assessment Methods And Object Examine: System and information and techniques documentation; info	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design bocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 Attions of compromise or potential compromise to the security of the information system; and is a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ts integrity policy; procedures addressing information system monitoring tools and techniques; information system security ormation system configuration settings and associated documentation; other relevant documents or records.(Optional	n documentation; information system other relevant documents or Related Controls:
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica (ii) the information system provides Assessment Methods And Object Examine: System and information and techniques documentation; info Test: Information system monitorin	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design bournentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 tions of compromise or potential compromise to the security of the information system; and is a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ts integrity policy; procedures addressing information system monitoring tools and techniques; information system securi ormation system configuration settings and associated documentation; other relevant documents or records.(Optional) areal-time alert capability.(Optional)	n documentation; information system other relevant documents or Related Controls:
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica (ii) the information system provides Assessment Methods And Object Examine: System and information and techniques documentation; info Test: Information system monitorin SI-4(CMS-1) – Enhancement (Low	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design bournentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 tions of compromise or potential compromise to the security of the information system; and is a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ts integrity policy; procedures addressing information system monitoring tools and techniques; information system securi ormation system configuration settings and associated documentation; other relevant documents or records.(Optional) areal-time alert capability.(Optional)	n documentation; information system other relevant documents or Related Controls:
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica (ii) the information system provides Assessment Methods And Object Examine: System and information and techniques documentation; infor Test: Information system monitorin SI-4(CMS-1) – Enhancement (Low Control	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design pocumentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 tions of compromise or potential compromise to the security of the information system; and is a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ts integrity policy; procedures addressing information system monitoring tools and techniques; information system security ormation system configuration settings and associated documentation; other relevant documents or records.(Optional) ()	n documentation; information system other relevant documents or Related Controls:
Assessment Methods And Object Examine: System and information monitoring tools and techniques do records.(Optional) Test: Information system-wide intru SI-4(5) – Enhancement (Low) Control Real-time alerts are provided when (a) Presence of malicious code, (b) Unauthorized export of informat (c) Signaling to an external informat (d) Potential intrusions. Applicability: All ASSESSMENT PROCEDURE: SI-4 Assessment Objective Determine if: (i) the organization identifies indica (ii) the information system provides Assessment Methods And Object Examine: System and information and techniques documentation; infor Test: Information system monitorin SI-4(CMS-1) – Enhancement (Low	ts integrity policy; procedures addressing information system monitoring tools and techniques; information system design bournentation; information system configuration settings and associated documentation; information system protocols; usion detection capability.(Optional) in indications of the following types of compromise, or potential compromise, occur: tion, ation system, or References: ARS: SI-4(5) 4(5).1 tions of compromise or potential compromise to the security of the information system; and is a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur. ts integrity policy; procedures addressing information system monitoring tools and techniques; information system securi ormation system configuration settings and associated documentation; other relevant documents or records.(Optional) areal-time alert capability.(Optional)	n documentation; information system other relevant documents or Related Controls:

ASSESSMENT PROCEDURE: SI-4(CMS-1).1

Assessment Objective

Determine if:

(i) IDS devices are installed at network perimeter points; and

(ii) host-based IDS sensors are installed on critical servers.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

Interview: Personnel with system and information integrity responsibilities to determine IDS devices are installed at network perimeter points and host-based IDS sensors are installed on critical servers.

SI-5 – Security Alerts and Advisories (Low)

Control

Procedures shall be developed, documented, and implemented effectively to establish a process for receiving IS alerts and advisories on a regular basis, and for issuing IS alerts and advisories to appropriate personnel. Upon receipt of such alerts and advisories, personnel shall take appropriate response actions. The types of actions to be taken in response to security alerts / advisories shall be documented.

Guidance

The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST SP 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Applicability: All	References: ARS: SI-5; NIST 800-53/53A: SI-5; PISP: 4.17.5	Related Controls:
ASSESSMENT PROCEDURE: SI-5.1		

Assessment Objective

Determine if:

(i) the organization receives information system security alerts/advisories on a regular basis;

(ii) the organization issues security alerts/advisories to appropriate organizational personnel; and

(iii) the organization takes appropriate actions in response to security alerts/advisories.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; NIST SP 800-40; records of security alerts and advisories; other relevant documents or records.

Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system. (Optional)

SI-7 – Software and Information Integrity (Low)

Control

Automated mechanisms for software and information integrity shall be in place and supporting procedures shall be developed, documented, and implemented effectively to both protect against and detect unauthorized changes to software. Good software engineering practices consistent with CMS IS policy and procedures shall be employed with regard to commercial-off-the-shelf (COTS) integrity mechanisms, and automated mechanisms shall be in place to monitor the integrity of the CMS information system and applications.

Guidance

The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Applicability: All	References: ARS: SI-7; FISCAM: TAN-3.1.2, TAN-3.2.1, TAN-3.2.2, TAY-2.1.4, TAY-2.2.2, TCP-	Related Controls:
	2.1.2, TCP-2.1.3, TCP-2.1.4; HIPAA: 164.312(c)(2), 164.312(e)(2)(i); NIST 800-53/53A: SI-7; PISP:	
	4.17.7	

ASSESSMENT PROCEDURE: SI-7.1

Assessment Objective

Determine if:

(i) the information system detects and protects against unauthorized changes to software and information; and

CMS	Core Security Requirements for Low Impac	ct Level Assessments
(ii) the organization employs effective integrity v	erification tools in accordance with good software engineering practices.	
Assessment Methods And Objects		
Examine: System and information integrity polic	cy; procedures addressing software and information integrity; information tools and applications documentation; other relevant documents or record	system design documentation; information system configuration settings and ds.(Optional)
Test: Software integrity protection and verification		
SI-7(FIS-1) – Enhancement (Low)		
Control		
	ata is developed that represents the various activities and conditions that	will be encountered in processing. Live data are not used in testing of
Applicability: All	References: FISCAM: TCC-2.1.6, TCC-2.1.7	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-1).1		
Assessment Objective		
Determine if:		
(i) the organization provides a comprehensive se	et of test transactions and data is developed that represents the various a e data in testing of program changes except to build test data files.	activities and conditions that will be encountered in processing.
Assessment Methods And Objects		
Examine: Pertinent policies and procedures.		
Examine: Test transactions and data.		
Interview: Programmers, auditors, and quality a	assurance personnel.	
SI-7(FIS-2) – Enhancement (Low)		
Control		
	stablished over source documents are used to help determine the comple	steness of data entry and processing
Applicability: All	References: FISCAM: TCP-1.1.1	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-2).1		
· · · · · · · · · · · · · · · · · · ·		
Assessment Objective		a of data anti- and management
	ecord count and control totals documents help determine the completenes	ss of data entry and processing.
Assessment Methods And Objects	and control totals	
Examine: Activity for developing record counts a Examine: Application documentation.	and control totals.	
Examine: Pertinent policies and procedures.		
Interview: User management and personnel.		
SI-7(FIS-3) – Enhancement (Low)		
Control	nd control totals are accumulated prograce well for a prosific time paried	(daily or more frequently) and are used to help determine the completeness
or data entry and processing.	nd control totals are accumulated progressively for a specific time period	(daily of more frequently) and are used to help determine the completeness
Applicability: All	References: FISCAM: TCP-112	Related Controls
Applicability: All ASSESSMENT PROCEDURE: SI-7(EIS-3) 1	References: FISCAM: TCP-1.1.2	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-3).1	References: FISCAM: TCP-1.1.2	Related Controls:
ASSESSMENT PROCEDURE: SI-7(FIS-3).1 Assessment Objective	•	
ASSESSMENT PROCEDURE: SI-7(FIS-3).1 Assessment Objective Determine if the organizational on-line or real-tin	me systems, record count and control totals are accumulated progressivel	ly for a specific time period (daily or more frequently) and are used to help
ASSESSMENT PROCEDURE: SI-7(FIS-3).1 Assessment Objective Determine if the organizational on-line or real-tin determine the completeness or data entry and p	me systems, record count and control totals are accumulated progressivel	
ASSESSMENT PROCEDURE: SI-7(FIS-3).1 Assessment Objective Determine if the organizational on-line or real-tin determine the completeness or data entry and p Assessment Methods And Objects	me systems, record count and control totals are accumulated progressivel	<u>.</u>
ASSESSMENT PROCEDURE: SI-7(FIS-3).1 Assessment Objective Determine if the organizational on-line or real-tin determine the completeness or data entry and p Assessment Methods And Objects Examine: Application documentation.	me systems, record count and control totals are accumulated progressivel	<u>.</u>
ASSESSMENT PROCEDURE: SI-7(FIS-3).1 Assessment Objective Determine if the organizational on-line or real-tin determine the completeness or data entry and p Assessment Methods And Objects Examine: Application documentation. Examine: Pertinent policies and procedures.	me systems, record count and control totals are accumulated progressivel processing.	
ASSESSMENT PROCEDURE: SI-7(FIS-3).1 Assessment Objective Determine if the organizational on-line or real-tin determine the completeness or data entry and p Assessment Methods And Objects Examine: Application documentation. Examine: Pertinent policies and procedures. Examine: Supporting documentation generated	me systems, record count and control totals are accumulated progressivel processing.	
ASSESSMENT PROCEDURE: SI-7(FIS-3).1 Assessment Objective Determine if the organizational on-line or real-tin determine the completeness or data entry and p Assessment Methods And Objects Examine: Application documentation. Examine: Pertinent policies and procedures.	me systems, record count and control totals are accumulated progressivel processing.	

SI-7(FIS-4) – Enhancement (Low)		
Control		
Record counts and control totals are	e established over and entered with transaction data, and reconciled to de	termine the completeness of data entry.
Applicability: All	References: FISCAM: TCP-2.1.1	Related Controls:
ASSESSMENT PROCEDURE: SI-7	(FIS-4).1	
Assessment Objective		
Determine if the organizational reco	rd counts and control totals are established over and entered with transact	tion data, and reconciled to determine the completeness of data entry.
Assessment Methods And Objects		
Examine: Application documentation	n.	
Examine: Pertinent policies and pro	ocedures.	
Examine: Reconciliation activities.		
Interview: Data control personnel.		
Interview: User management and p	ersonnel.	
SI-7(FIS-5) – Enhancement (Low)		
Control		
Reconciliations are performed to de	termine the completeness of transactions processed, master files update	d, and outputs generated.
Applicability: All	References: FISCAM: TCP-2.2.1	Related Controls:
ASSESSMENT PROCEDURE: SI-7	(FIS-5).1	
Assessment Objective		
	nciliations are performed to determine the completeness of transactions	processed, master files updated, and outputs generated.
Assessment Methods And Object		······································
Examine: Application documentation		
Examine: Pertinent policies and pro		
Examine: Reconciliation activities.		
Interview: Data control personnel.		
Interview: User management and p	ersonnel.	
SI-8 – Spam Protection (Low)		
Control		
Automated mechanisms for spam p	rotection shall be in place at critical information system entry points, work	stations, servers, and mobile computing devices on the network. Supporting procedures
	nd implemented effectively to both protect against and detect spam.	
Guidance		
The organization employs spam pro	tection mechanisms at critical information system entry points (e.g., firew	alls, electronic mail servers, remote-access servers) and at workstations, servers, or
		and take appropriate action on unsolicited messages transported by electronic mail,
		m protection software products from multiple vendors (e.g., using one vendor for
	another vendor for workstations). NIST SP 800-45 provides guidance on	
Applicability: All	References: ARS: SI-8; HIPAA: 164.308(a)(1)(i); NIST 800	-53/53A: SI-8; PISP: 4.17.8 Related Controls:
ASSESSMENT PROCEDURE: SI-8	.1	
Assessment Objective		
Determine if:		
(i) the information system implement		
	protection mechanisms at critical information system entry points and at w	
	protection mechanisms to detect and take appropriate action on unsolicit	5 I J
	protection mechanisms whenever new releases are available in accordar	ce with organizational policy and procedures.
Assessment Methods And Object		
		m design documentation; spam protection mechanisms; information system configuration
	tion; other relevant documents or records.(Optional)	
Test: Spam detection and handling		
Rev. 9	Page 124 of 127	BPSSM Appendix A. Attachment 3

SI-12 – Information Output Handling and	d Retention (Low)	
Control		
	ed and retained in accordance with applicable laws, Executive Orders, directives, policies, regulation	ons, standards, operational requirements, and the
Guidance		
A good place to obtain procedures for handling	sensitive output information is the NIST SP.	
Applicability: All	References: ARS: SI-12; FISCAM: TAY-4.1.6; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2; NIST 800-53/53A: SI-12; PISP: 4.17.12	Related Controls:
ASSESSMENT PROCEDURE: SI-12.1	•	
Assessment Objective		
Determine if:		
 (i) the organization handles and retains output fr requirements; and 	om the information system in accordance with applicable laws, Executive Orders, directives, polici	es, regulations, standards, and operational
not limited to, special instructions for disseminat	rmation system in accordance with labeled or marked instructions on information system output (ir ion, distribution, transport, or storage of information system output.	ncluding paper and digital media) that includes, but
Assessment Methods And Objects		
Examine: System and information integrity polic	cy; procedures addressing information system output handling and retention; media protection policity;	cy and procedures; information retention records,
other relevant documents or records.(Optional)	ation output handling and retention responsibilities.(Optional)	
SI-12(CMS-1) – Enhancement (Low)		
Control	records, system reports, business and financial reports, and business records, from the information	n avetam in accordance with CMS Baliay and all
applicable National Archives and Records Admi	nistration (NARA) requirements.	is system in accordance with CMS Policy and all
Applicability: All	References: ARS: SI-12(1); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2	Related Controls:
ASSESSMENT PROCEDURE: SI-12(CMS-1).		Related Controls:
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective	1	
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I	uding, but not limited to audit records, system reports, business and financial reports, and busines	
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects	uding, but not limited to audit records, system reports, business and financial reports, and busines NARA requirements.	s records, from the information system in
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for reco	uding, but not limited to audit records, system reports, business and financial reports, and busines	s records, from the information system in
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for reco	uding, but not limited to audit records, system reports, business and financial reports, and busines NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t	s records, from the information system in
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for reco Policy and all applicable National Archives and I	uding, but not limited to audit records, system reports, business and financial reports, and busines NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t	s records, from the information system in
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for recc Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all outp processing control group: (1) has a schedule by	uding, but not limited to audit records, system reports, business and financial reports, and business NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met.	s records, from the information system in from the information system in accordance with CMS
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for recc Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all outprocessing control group: (1) has a schedule by reviews output products for general acceptability	uding, but not limited to audit records, system reports, business and financial reports, and business NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met. outs are produced and distributed according to system requirements and design by a data process application that shows when outputs should be completed, when they need to be distributed, who <i>r</i> ; and (3) reconciles control information to determine completeness of processing.	is records, from the information system in from the information system in accordance with CMS sing control group, or some alternative. A data the recipients are, and the copies needed; (2)
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for recc Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all outprocessing control group: (1) has a schedule by reviews output products for general acceptability Applicability: All	uding, but not limited to audit records, system reports, business and financial reports, and business NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met.	s records, from the information system in from the information system in accordance with CMS
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for rec Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all out processing control group: (1) has a schedule by reviews output products for general acceptability Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS-1).1	uding, but not limited to audit records, system reports, business and financial reports, and business NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met. outs are produced and distributed according to system requirements and design by a data process application that shows when outputs should be completed, when they need to be distributed, who <i>r</i> ; and (3) reconciles control information to determine completeness of processing.	is records, from the information system in from the information system in accordance with CMS sing control group, or some alternative. A data the recipients are, and the copies needed; (2)
ASSESSMENT PROCEDURE: SI-12(CMS-1). ⁻ Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for rec Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all outprocessing control group: (1) has a schedule by reviews output products for general acceptability Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS-1).1 Assessment Objective	uding, but not limited to audit records, system reports, business and financial reports, and busines NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met. puts are produced and distributed according to system requirements and design by a data process application that shows when outputs should be completed, when they need to be distributed, who <i>r</i> ; and (3) reconciles control information to determine completeness of processing. References: FISCAM: TAY-4.1.1, TAY-4.1.2	is records, from the information system in from the information system in accordance with CMS sing control group, or some alternative. A data the recipients are, and the copies needed; (2) Related Controls:
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for rec Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all outprocessing control group: (1) has a schedule by reviews output products for general acceptability Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS-1).1 Assessment Objective Determine if the organization assigns responsib alternative. A data processing control group: (1)	uding, but not limited to audit records, system reports, business and financial reports, and business NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met. outs are produced and distributed according to system requirements and design by a data process application that shows when outputs should be completed, when they need to be distributed, who <i>r</i> ; and (3) reconciles control information to determine completeness of processing.	is records, from the information system in from the information system in accordance with CMS sing control group, or some alternative. A data the recipients are, and the copies needed; (2) Related Controls: design by a data processing control group, or some
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for rec Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all outprocessing control group: (1) has a schedule by reviews output products for general acceptability Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS-1).1 Assessment Objective Determine if the organization assigns responsib alternative. A data processing control group: (1)	uding, but not limited to audit records, system reports, business and financial reports, and business NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met. outs are produced and distributed according to system requirements and design by a data process application that shows when outputs should be completed, when they need to be distributed, who r; and (3) reconciles control information to determine completeness of processing. References: FISCAM: TAY-4.1.1, TAY-4.1.2	is records, from the information system in from the information system in accordance with CMS sing control group, or some alternative. A data the recipients are, and the copies needed; (2) Related Controls: design by a data processing control group, or some
ASSESSMENT PROCEDURE: SI-12(CMS-1). Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for rec Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all outprocessing control group: (1) has a schedule by reviews output products for general acceptability Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS-1).1 Assessment Objective Determine if the organization assigns responsib alternative. A data processing control group: (1) needed; (2) reviews output products for general	uding, but not limited to audit records, system reports, business and financial reports, and business NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met. outs are produced and distributed according to system requirements and design by a data process application that shows when outputs should be completed, when they need to be distributed, who r; and (3) reconciles control information to determine completeness of processing. References: FISCAM: TAY-4.1.1, TAY-4.1.2	is records, from the information system in from the information system in accordance with CMS sing control group, or some alternative. A data the recipients are, and the copies needed; (2) Related Controls: design by a data processing control group, or some
ASSESSMENT PROCEDURE: SI-12(CMS-1).* Assessment Objective Determine if the organization retains output, incl accordance with CMS Policy and all applicable I Assessment Methods And Objects Examine: At a minimum, documentation for recc Policy and all applicable National Archives and I SI-12(FIS-1) – Enhancement (Low) Control Responsibility is assigned for seeing that all outprocessing control group: (1) has a schedule by reviews output products for general acceptability Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS-1).1 Assessment Objective Determine if the organization assigns responsible alternative. A data processing control group: (1) needed; (2) reviews output products for general Assessment Methods And Objects	uding, but not limited to audit records, system reports, business and financial reports, and business NARA requirements. ord retention audit records, system reports, business and financial reports, and business records, t Records Administration (NARA) requirements are met. outs are produced and distributed according to system requirements and design by a data process application that shows when outputs should be completed, when they need to be distributed, who r; and (3) reconciles control information to determine completeness of processing. References: FISCAM: TAY-4.1.1, TAY-4.1.2	is records, from the information system in from the information system in accordance with CMS sing control group, or some alternative. A data the recipients are, and the copies needed; (2) Related Controls: design by a data processing control group, or some

Operational		
Control		
Printed reports contain a title page with rep	port name, time and date of production, the processing period covered; and hav	/e an "end-of-report" message.
Applicability: All	References: FISCAM: TAY-4.1.3	Related Controls:
ASSESSMENT PROCEDURE: SI-12(FIS-	2).1	
Assessment Objective	_,	
	system printed reports contain a title page with report name, time and date of p	production, the processing period covered: and have an "end-of-report"
message.	system printed reports contain a the page with report name, time and date of p	production, the processing period covered, and have all one of report
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Printed reports.		
Interview: User personnel and application	programmer, if available.	
SI-12(FIS-3) – Enhancement (Low)		
Control		
Each output produced, whether printed or t	transmitted to a user's terminal device, is logged, manually if not automatically,	including the recipient(s) who receive the output.
Applicability: All	References: FISCAM: TAY-4.1.4, TAY-4.1.5	Related Controls:
ASSESSMENT PROCEDURE: SI-12(FIS-	-3).1	
Assessment Objective		
Determine if the organizational information	system's output produced, whether printed or transmitted to a user's terminal of	device, is logged, manually if not automatically, including the recipient(s) who
receive the output.		
Assessment Methods And Objects		
Examine: Application documentation.		
Examine: Output logs.		
Interview: Information system and user pe	ersonnel.	
SI-12(FIS-4) – Enhancement (Low)		
Control		
In the user department, outputs transmitted	d are summarized daily and printed for each terminal device, and reviewed by s	supervisors. A control log of output product errors is maintained, including th
In the user department, outputs transmitted corrective actions take.		
In the user department, outputs transmitted corrective actions take. Applicability: All	References: FISCAM: TAY-4.1.7, TAY-4.1.8	supervisors. A control log of output product errors is maintained, including th Related Controls:
In the user department, outputs transmitted corrective actions take.	References: FISCAM: TAY-4.1.7, TAY-4.1.8	
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective	References: FISCAM: TAY-4.1.7, TAY-4.1.8	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 system's user department, outputs transmitted are summarized daily and printer	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 system's user department, outputs transmitted are summarized daily and printer	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includie	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 In system's user department, outputs transmitted are summarized daily and printed ing the corrective actions take.	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includin Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g.,	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 In system's user department, outputs transmitted are summarized daily and printed ing the corrective actions take.	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includie Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity.	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 I system's user department, outputs transmitted are summarized daily and printering the corrective actions take. ES.	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includii Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity. Interview: User supervisory personal.	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 I system's user department, outputs transmitted are summarized daily and printering the corrective actions take. ES.	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includie Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity.	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 I system's user department, outputs transmitted are summarized daily and printering the corrective actions take. ES.	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includii Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity. Interview: User supervisory personal.	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 I system's user department, outputs transmitted are summarized daily and printering the corrective actions take. ES.	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includi Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity. Interview: User supervisory personal. SI-12(FIS-5) – Enhancement (Low) Control	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 I system's user department, outputs transmitted are summarized daily and printering the corrective actions take. ES.	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includii Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity. Interview: User supervisory personal. SI-12(FIS-5) – Enhancement (Low) Control Users review output reports for data accuration (5) control totals balance reports. Output for	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 - system's user department, outputs transmitted are summarized daily and printering the corrective actions take. - es. , printed daily summaries with supervisory initials or signatures).	Related Controls: ed for each terminal device, and reviewed by supervisors. A control log of action reports, (3) master record change reports, (4) exception reports, and
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includii Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity. Interview: User supervisory personal. SI-12(FIS-5) – Enhancement (Low) Control Users review output reports for data accura (5) control totals balance reports. Output fr Applicability: All	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 a system's user department, outputs transmitted are summarized daily and printering the corrective actions take. es. , printed daily summaries with supervisory initials or signatures). acy, validity, and completeness. The reports include: (1) error reports, (2) transation reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1	Related Controls:
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includii Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity. Interview: User supervisory personal. SI-12(FIS-5) – Enhancement (Low) Control Users review output reports for data accuration (5) control totals balance reports. Output for	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 a system's user department, outputs transmitted are summarized daily and printering the corrective actions take. es. , printed daily summaries with supervisory initials or signatures). acy, validity, and completeness. The reports include: (1) error reports, (2) transation reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1	Related Controls: ed for each terminal device, and reviewed by supervisors. A control log of action reports, (3) master record change reports, (4) exception reports, and
In the user department, outputs transmitted corrective actions take. Applicability: All ASSESSMENT PROCEDURE: SI-12(FIS- Assessment Objective Determine if the organizational information output product errors is maintained, includii Assessment Methods And Objects Examine: Pertinent policies and procedure Examine: Supporting documentation (e.g., Examine: This activity. Interview: User supervisory personal. SI-12(FIS-5) – Enhancement (Low) Control Users review output reports for data accura (5) control totals balance reports. Output fr Applicability: All	References: FISCAM: TAY-4.1.7, TAY-4.1.8 -4).1 a system's user department, outputs transmitted are summarized daily and printering the corrective actions take. es. , printed daily summaries with supervisory initials or signatures). acy, validity, and completeness. The reports include: (1) error reports, (2) transation reruns is subjected to the same quality review as the original output. References: FISCAM: TAY-4.1.9, TAY-4.2.1	Related Controls: ed for each terminal device, and reviewed by supervisors. A control log of action reports, (3) master record change reports, (4) exception reports, and

reports, (4) exception reports, and (5) control totals balance reports. Output from reruns is subjected to the same quality review as the original output.

Assessment Methods And Objects

Examine: Activity to review output reports. Examine: Output reports. Examine: Pertinent policies and procedures. Interview: User management and personnel.

Appendix B: Medicare Information Technology (IT) Systems Contingency Planning

Table of Contents

(Rev. 9, 06-20-08)

- 1 Introduction
- 2 Scope
- 3 Definition of an Acceptable Contingency Plan
- 4 Medicare IT Systems Contingency Planning
 - 4.1 Contingency Planning
 - 4.2 Coordination with Other Business Partners
- 5 Medicare IT Systems Contingency Plan
- 6 Testing
 - 6.1 Claims Processing Data Centers
 - 6.2 Multiple Contractors
 - 6.3 Test Types
 - 6.3.1 Live vs. Walkthrough
 - 6.3.2 End-to-End
 - 6.4 Local Processing Environments (PCs/LANs)
 - 6.5 Test Planning
- 7 Minimum Recovery Times
- 8 Responsibilities
 - 8.1 Business Partner Management
 - 8.2 Systems Security Officer (SSO)
 - 8.3 Service Components (provide support functions such as maintenance,

physical security)

8.4 Operating Components (IT operations personnel)

- 9 Changes
- 10 Attachments
- 11 Checklist
- 12 References

1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS business partners are required by CMS CSR 5.2 to develop and maintain a contingency plan. This plan is to provide information to aid the business partner in planning for and responding to an emergency or system disruption, and to recover from that emergency or disruption.

Section 3.4 of this document requires that all CMS Medicare business partners prepare, review, and test their Medicare IT systems contingency plans. All General Support Systems (GSS) and Major Applications (MA) that support critical Medicare operations *shall* be covered by a Medicare IT Systems Contingency Plan (CP).

This document presents the direction for accomplishing Medicare IT systems contingency planning. It is to be used by the CMS Medicare business partner management, IT systems management and staff, and system security persons charged with preparing for continuing the operation of Medicare systems and developing an IT systems contingency plan, or updating an existing plan.

The business partner information security risk assessment may be used as a checkpoint to determine if appropriate contingencies have been addressed in the contingency plan.

To ensure the contingency plan is workable, it *shall* be thoroughly and periodically tested.

The simplified diagram in Figure B-1 illustrates the IT systems contingency planning process.

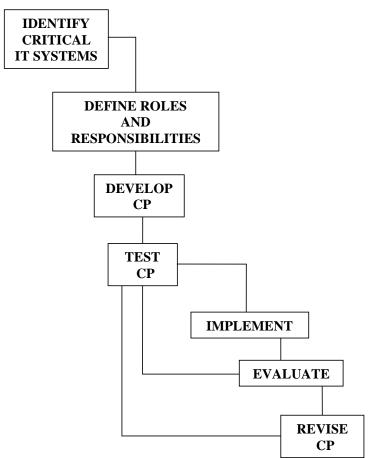


Figure B-1 – IT Systems Contingency Planning Process

3 Definition of an Acceptable Contingency Plan (*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

A contingency plan is a document that describes how to plan for and deal with an emergency or system disruption. These situations could be caused by a power outage, hardware failure, fire, or terrorist activity. A contingency plan is developed and maintained to ensure quick, appropriate, effective, and efficient response in those situations for which a foreseen risk cannot be mitigated or avoided.

Protecting lives is the paramount task while executing a contingency plan.

Before developing an IT systems contingency plan, it is advisable to have or create a contingency policy. The contingency plan *shall* be driven by a contingency policy. The contingency policy is a high level statement relative to what the management wants to do to address a contingency and to recover from the emergency or system disruption.

The IT systems contingency plan *shall* be developed under the guidance of IT management and systems security persons and all organizational components *shall* be

actively involved in providing information for developing the plan, for making plan related decisions, and for providing support to plan testing.

It can be a very subjective argument relative to what constitutes an acceptable contingency plan. In this document, the description of an acceptable contingency plan is based on the results of the research, analysis and review of various documents from Government and industry, and the review of existing business partner contingency plans and test reports.

The following summary statements define what constitutes an acceptable contingency plan. This is not an all-inclusive list and the topics are not in any order of importance or priority.

- 1. Considers the protection of human life as the paramount guiding principle, and then aims at the backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high-quality service.
- 2. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.
- 3. Considers risk assessment results.
- 4. Addresses possible and probable emergencies or system disruptions.
- 5. Can be sufficiently tested on an established regular basis at reasonable cost.
- 6. Contains information that is needed and useful during an emergency or system disruption.
- 7. Can, when implemented, produce a response and recovery, such that critical business functions are continued.
- 8. Specifies the persons necessary to implement the plan, and clearly defines their responsibilities.
- 9. Clearly defines the resources necessary to implement the plan.
- 10. Reflects what can be done is not a wish list.
- 11. Assumes people *shall* use sound judgment, but will need clearly stated guidance, since they will be functioning in a non-normal environment, under possibly severe pressure.
- 12. Addresses backup and alternate sites.
- 13. Addresses the use of manual operations, where appropriate and necessary.

14. Contains definitive "Call Lists" to use for contacting the appropriate persons in the proper sequence. This list would include vendor points of contact.

An acceptable contingency plan should be straight to the point. It should not contain any more information than is necessary to plan for and implement contingency actions. The users should not get bogged down in detail as they read the plan to determine what to do, when to do it, what is needed to do it, and who should do it. The contingency plan should serve as a "user's manual" and be easy to understand and use.

Because a contingency plan is designed to be used in a stressful situation, it *shall* be written with that as a foremost thought in mind. The prime objective is to maximize the continuity of critical operations.

Reviewing a contingency plan and testing it will help determine whether it remains an acceptable plan. The review and testing *shall* not focus solely on content, but *shall* also focus on ease of use.

A complete set of contingency plans for an organization may be made up of several smaller contingency plans, one for each business function (e.g. claims processing) or for a single data center, for example. This breakdown into manageable parts helps to keep a plan easy to use.

Careful thought should be given to the organization of the contingency plan. The organization should be logical in terms of what will the user want to know or do first. If the first thing that should happen in an emergency is that a call list *shall* be used to notify persons, then that call list, or a pointer to it, should be placed very near the front of the contingency plan. Not every informational item to be utilized during a contingency event will be in the contingency plan document. For example, the plan may point to an attachment or to a separate procedures manual. In this regard, a contingency plan should contain a very understandable and useful table of contents, so that a user can quickly find the information being sought.

Contingency planning can provide a cost-effective way to ensure that critical IT capabilities can be recovered quickly after an emergency. IT systems contingency planning *shall* embrace a coordinated contingency policy of what will be done to fully recover and reconstitute all operations.

4.1 Contingency Planning

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Contingency planning is preparing for actions in the event of an emergency situation, and giving some thought and planning to what your organization will do to respond and recover. The IT systems contingency planning process *shall* address all the actions and resources needed to ensure continuity of operation of critical Medicare IT systems and the means of implementing the needed resources. IT management and staff *shall* be

trained to handle emergency or system disruption situations in data centers and other areas where data processing systems are located. Contingency planning includes such training.

It is advisable to establish a Medicare IT systems contingency planning team. This team would be responsible for defining critical Medicare IT systems, including applications software, data, processing and communications capabilities, and other supporting resources. These would be the key people in the implementation of the plan.

4.2 Coordination with Other Business Partners

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

If a business partner's data center or other data processing environment is linked to other business partners for the transmission of Medicare data, then the contingency planning *shall* include those links relative to receiving input, exchanging files, and distributing output. If alternate/backup IT systems capabilities are to be utilized, then their functions and data transmission links *shall* be considered in the planning.

Coordination with other business partners is essential to completing the IT systems contingency planning process.

5 Medicare IT Systems Contingency Plan

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The following format may be used in developing an IT system contingency plan. While this format is not required, all of its elements *shall* be included in the Contingency Plan.

- 1. Introduction
 - Background
 - Purpose/Objective
 - Management commitment statement
 - Scope
 - Organizations
 - o Systems
 - o Boundaries
 - IT capabilities and resources
 - CP policy
 - Priorities
 - Continuous operation
 - Recovery after short interruption
 - Minimum recovery times
- 2. Assumptions
- 3. Authority/References

- 4. Definition of what the CP addresses
 - Organizations
 - Systems
 - Boundaries
- 5. Three phases defined
 - Respond
 - Recover
 - Restore/reconstitute
- 6. Roles/Responsibilities defined
- 7. Definition of critical functions
- 8. Alternate capabilities and backup
- 9. Definition of required resources to respond and recover
- 10. Training
 - CP *shall* address Who When How
- 11. Testing the CP
 - Philosophy
 - Plans
 - Boundaries
 - Live vs. Walkthrough
 - Reports
 - Responsibilities
- 12. CP maintenance/updating
 - Schedule
- 13. Relationships/Interfaces
 - Outside (vendors, providers, banks, utilities, services, CMS)
 - Internal
 - Dependencies
- 14. Attachments
 - Actions for each phase
 - Procedures
 - Call trees
 - Vendor contact list
 - Hardware inventory
 - Software inventory

- System descriptions
- Alternate/Backup site information
- Assets/Resources
- Risk Assessment Summary (refer to System Security Plans)
- Agreements/Memos of Understanding
- Manual Operations
- Supplies/Materials/Equipment
- Floor plans
- Maps

The contingency plan *shall* provide for off-site storage:

- Backup software
- Data
- Appropriate documents (emergency telephone lists, memos of understanding, etc.)
- Copies of the contingency plan
- Administrative supplies (forms, blank check stock, etc.)

6 Testing

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

CMS requires testing of the contingency plan annually under conditions that simulate an emergency or a disaster. A contingency plan shall also be tested after a substantive system change that necessitates a revision to the contingency plan.

CMS requires that the critical IT systems *shall* be tested annually and the contingency plan updated to accommodate any changes, including updated versions of software or critical data. Critical systems are those whose failure to function, for even a short time, could have a severe impact, or have a high potential for fraud, waste, or abuse.

6.1 Claims Processing Data Centers

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Many of the contractors with which CMS has direct contracts do not have their own data centers. They usually contract this service out. If a business partner does not have its own data center, then it is the responsibility of the business partner to inform the subcontractor that operates the data center that they *shall* have a contingency plan.

6.3 Test Types

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Contingency plan test guidance suggests *four (4)* types of testing:

• Walkthrough

- Simulation/modeling
- Tabletop Test
- Live

These are defined below:

- Walkthrough: A walkthrough test is accomplished by going through a set of steps to accomplish a particular task or action initiated because of a contingency event. The precursor to a walkthrough test is that the steps are documented so that they can be logically followed. A "test team" might sit around a table and talk through each step and then walk through" the various steps, and then discuss expected outcomes and further actions to be taken. They may use a checklist to ensure that all features of a step are addressed or that all resources necessary to accomplish the task or action are considered. A walkthrough test does not involve accomplishing the actions being tested in real time or using the live environment. A walkthrough test could be accomplished by using a group of test people to act out what might happen if a real contingency event occurred. They might go to the alternate site, but they would not actually start all hardware, software, and communication operations in order to assume the function of the primary site.
- **Simulation/Modeling**: Modeling involves creating a computer model of the process to be tested. This allows easy testing of many variables without physically having to make changes. For example, you can vary the number of servers that go down during a disaster or the number of people that can get to an alternate site following a disaster.

Simulation involves taking physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team does the same at the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.

• **Tabletop Test**: For those applications that are both hosted at CMS <u>and not</u> participating in a broader recovery test to a CMS-approved recovery site during their annual test cycle, a tabletop test is required. A tabletop test is discussion-based only, and does not involve deploying equipment or other resources. The discussion during the test can be based on a single scenario or multiple scenarios. By simulating an emergency in an informal, stress-free environment, this test method allows for the free exchange of ideas and provides participants an opportunity to practice the steps to be followed in an actual event and to identify areas in the contingency plan for enhancement.

A successful tabletop test steps participants through real-life scenarios; captures its results in a formal report; and incorporates the "lessons learned" into subsequent versions of the contingency plan and the tabletop test plan. Refer to

CMS Contingency Planning Tabletop Test Procedures, for step-by-step instructions for conduction a tabletop test.

• Live: This is the most complete and expensive test to accomplish. It involves completing the physical steps that would actually be taken if an emergency occurred. People and materials would be moved to an alternate site for the test, and servers would actually be shut down to reduce capability. Power would be shut off, and live conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications, and people at the alternate site would be set into action and begin functioning as the primary site to support operations.

End-to-end refers to the scope of the testing (partial testing is less than end-to-end). When conducting end-to-end testing, items to consider include:

- End-to-end testing can be completed as part of walkthrough or live test.
- Not testing end-to-end means that some links, processes, or subsystems are missed.
- What is the risk in not conducting end-to-end testing?
- Live end-to-end testing can be very expensive!

Considering risks and cost, management *shall* make a decision as to what type and scope of testing is appropriate.

6.3.1 Live vs. Walkthrough

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

- High-level testing can take the form of a walkthrough test.
- A walkthrough can be part of the overall testing process, but not the whole process.
- Lower-level testing can include a walkthrough, if live testing is not an option.
 - Live testing *shall* be the first choice.
 - Fall back to a simulation/model if live testing is not an option.
 Cost, time, and interruption of normal operations are major considerations in doing a live test.
 - A walkthrough test should be the last resort.
- Ask what a walkthrough test would miss.

- Consider the ramifications of missing that part of the test.
- Remember that there is risk in not doing a live test—can the risk be accepted?
 - Consider the criticality of functions, processes, and systems.
 If critical to continuing essential business operations, then these are strong candidates for live testing.
- Testing interfaces.

It is important to test the critical interfaces with internal and external systems. It is difficult to test interfaces using a "walkthrough" method. Simulation or "live" testing is preferred.

• Cost and complexity.

The decision as to how to test critical functions, processes, and systems must result from careful consideration of complexity and cost. A complete "live" test of all elements of an operation may prove to be extremely costly, in terms of both dollars and time. If that cost out weighs the "cost" of the risk of not doing live testing, then "live" testing should probably be ruled out.

6.3.2 End-to-End

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This kind of testing aims to ensure that all software and hardware components associated with a function, process, or system are tested from the front end through to the back end (input through process through output). As with live testing, end-to-end testing can be expensive.

- End-to-end testing *shall* only be considered for critical functions, processes, or systems.
- Why is end-to-end testing needed? It provides the best assurance that there are no problems.
- Would a partial test be meaningful? If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical ones need be considered for end-to-end testing.
- Examples of types of end-to-end tests:
 - Claims receipt through to check generation
 - Query of a database through to the response
 - MSP check request through to check issue and back to MSP
- Evaluate complexity and cost.

The decision on how to test critical functions, processes, and systems *shall* carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and

time. If that cost out weighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.

- Consider the criticality of functions, processes, and systems. Look at the criticality of functions, processes, and systems. If these are critical to continuing essential business operations, then these are strong candidates for end-to-end testing.
- If you cannot do end-to-end testing, then consider live testing of all links possible to help ensure minimum problems.
 - Or, do simulation/modeling
 - Or, do walkthrough

Overall testing may take the form of reviews, analyses, or simulations of contingencies. Reviews and analyses may be used for non-critical systems, whereas critical systems *shall* be tested under conditions that simulate an emergency or a disaster.

It is advisable that the testing of critical systems be done end-to-end, input through output, so that no physical activity, automated process, or Medicare business partner system is left untested. Critical interfaces internal and external to the systems *shall* be tested.

Testing may include activities in addition to computer processing. Manual operations *shall* be checked according to procedures, and changes made as experience indicates.

6.4 Local Processing Environments (PCs/LANs)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

IT systems contingency plan testing relative to local environments, such as individual or clustered workstations and LAN configurations, may be less comprehensive than data center testing. Reviews and analyses may be used to accomplish certain non-critical systems testing, whereas critical systems require full simulation or live testing. The criticality of the system is the deciding factor relative to what type testing is used, how often tests are accomplished, and how thorough the testing *shall* be.

The decision of which test approach to use relative to a specific system or configuration *shall* be a management decision based on advice from the SSO, IT systems staff, operations and support representatives, and the lead test planner/manager.

6.5 Test Planning

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

An IT systems contingency test plan *shall* address at least the following:

- Test objectives
- Test approach

- Required equipment and resources
- Necessary personnel
- Schedules and locations
- Test procedures
- Test results
- Failed tests
- Corrective action management process
- Retest
- Approvals

It is advisable to establish test teams responsible for preparing and executing the IT systems contingency plan tests. Responsibilities *shall* be assigned to test team members, including executives, observers, and contractors.

Following testing, the corrections specified in a Corrective Action Management Process *shall* be tested. The process *shall* include:

- List of items that failed the previous test
- Corrections planned
- Retest detail
- Schedule
- Review responsibilities

Ensure that the lessons learned from IT systems contingency plan testing are discussed among senior business partner management, operations, IT management and staff, and the SSO.

Documentation *shall* exist for:

- Test plans
- Test results
- Corrective action management process
- Retest plans
- Memos of Understanding/Formal Test Arrangements

7 Minimum Recovery Times

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Recovery time is the time it takes to recover an operation, function, process, program, file, or whatever has to be recovered as an operational entity.

Minimum recovery time is the longest acceptable period of time for recovery of operations. If claims processing operations must be recovered within 72 hours, then that is the minimum acceptable time to recover. Anything over that is unacceptable.

- Recovery times *shall* vary, depending on the criticality of the entity involved.
- Times can be from a few minutes to days or weeks.
- A table/matrix can be constructed that lists the recovery times.
- There can be a separate table/matrix for each organization or major function (e.g., claims processing, medical review, check generation).
- Recovery times *shall* be carefully defined and must be achievable.
- Recovery times can be verified to some extent through testing (simulation or live).

8.1 Business Partner Management

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

- Defines scope and purpose of IT systems contingency planning.
- Authorizes preliminary IT systems contingency planning.
- Ensures that appropriate contingency plans are developed, periodically tested, and maintained.
- Ensures that all IT operations participate in the contingency planning and the development of the plans.
- Reviews the plan and recommendations.
- Requests and/or provides funds for plan development and approved recommendations.
- Assigns teams to accomplish development of test procedures, and for testing the plan.
- Reviews test results.
- Ensures that the appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are ready for use in the event of a disruption.
- Ensures that the business partner organization can demonstrate the ability to provide continuity of critical IT systems operation in the event of an emergency.
- Business partner management *shall* approve:

- The Contingency Plan
- o Changes to the Contingency Plan
- o Test Plans
- o Test results
- Corrective action management processes
- o Retest Plans
- o Memos of Understanding/Formal Arrangement Documents
- o Changes to storage and backup/alternate site facilities

9 Changes

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The contingency plan *shall* be updated whenever one or more of the following events occurs:

- New systems or operations added.
- Upgrade or replacement of Standard System software.
- Hardware or software replacement.
- Changed back up/alternate site.
- Changed storage facilities.
- Removal of existing systems or operations.

10 Attachments

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Materials that are too extensive to be included in the body of the Medicare IT systems contingency plan *shall* be included as attachments. These *shall* be referenced in the contingency plan. These *shall* also be a part of the Site Security Profile (Refer to CSR Category 1). Existing material that facilitates response, backup, and recovery operations *shall* be included as attachments or a pointer provided. Much of this material is bulky and relates to the entire organization. The SSO *shall* ensure that the information to be attached is pertinent and current, and that updated copies are routinely incorporated, particularly into offsite copies of the contingency plan. Such material includes:

- Master inventories of forms, supplies, and equipment
- Description of computer hardware and peripherals
- Description of applications software
- Appropriate security weakness information
- Systems and program documentation
- Prioritized schedules for computer operations
- Communications requirements, especially computer networks

11 Checklist

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The following checklist provides a means for determining if a contingency plan contains the appropriate information that can readily be used in handling an emergency or system disruption. This list is not all-inclusive, but rather should serve as a thought stimulus for evaluating contingency plans.

This checklist uses the same outline as the suggested contingency plan format.

- 1. Introduction Does the contingency plan contain:
 - Background Is a history of the plan provided? Are the physical environment and the systems discussed?
 - Purpose/Objective What does the plan address? Why was it written? What does it aim to accomplish?
 - Management Commitment Statement Has the contingency plan been approved by management and the SSO? Once the contingency plan is created, reviewed, and ready for distribution, it *shall* be approved by site, operations and information systems management, and the SSO.
 - Scope

Are the boundaries of the plan indicated? What organizations are involved, not involved?

- o Organizations
- o Systems
- o Boundaries
- IT Capabilities and Resources Is the focus of the plan on IT systems, capabilities, and resources?
- Contingency Plan Policy
 - o Priorities
 - Are the contingency plan steps ranked according to priority?
 - Continuous Operation
 - Are there functions, processes, or systems that are required to continue without interruption?

- o Recovery after Short Interruption
 - Which functions, processes, or systems can be interrupted for a short time?
- Recovery Times?
 - Are the recover times stated?
 - What are the minimum recovery times?
- Standalone Units
 - Does a contingency plan exist for any standalone workstation? A key part of a contingency plan *shall* address any standalone workstations that are part of the critical operations environment. It *shall* state where backup software and support data for these workstations is stored.
 - Is the plan reviewed and approved by other key affected persons?

2. Assumptions

Are all the important assumptions listed? Have the assumptions been carefully reviewed by the appropriate persons to ensure their validity?

- 3. Authority/References
 - Who or what document is authorizing the creation of the contingency plan?
 - What are the key references that apply to the plan?
- 4. Definition of what the Contingency Plan Addresses
 - Organizations To which organizations does the contingency plan apply?
 - Systems Is there a general description of systems and/or processes?
 - Boundaries Are the system boundaries clearly defined?
- 5. Three phases defined

Does the plan address three phases of emergency or system disruption?

- Respond
 - Is this phase adequately described so that it is understood what activities occur therein?
 - Is damage/impact assessment considered?
 - Are the alerting and initial impact assessment procedures fully explained as well as arrangements for continual review of their use and effectiveness?
- Recover

Is this phase adequately described so that it is understood what activities occur during this phase?

- Restore/Reconstitute Is this phase adequately described so that it is understood what activities occur during this phase?
- 6. Roles/Responsibilities Defined
 - Has the necessary contingency plan implementation organization been defined and the responsibilities of all those involved clearly stated with no 'gray areas'?
 - Will all who have a task to perform be aware of what is expected of them?
 - Does the contingency plan assign responsibilities for recovery? The responsibilities of key management and staff persons *shall* be carefully described in the contingency plan, so that there is no question relative to the duties of these people during an emergency.
- 7. Definition of Critical Functions
 - Does the contingency plan address critical systems and processes?
 - Have emergency processing priorities been established and approved by management?
 - Does the contingency plan specify critical data? The contingency plan *shall* specify the critical data needed to continue critical business functions and how frequently the data is backed up.
 - Has a list of critical operations, data, and applications been created? In preparation for preparing the contingency plan, a list of current critical operations, data and applications *shall* be prepared and approved by management. This list *shall* contain the items needed to continue the critical business functions until operations could be returned to a normal mode.
- 8. Alternate Capabilities and Backup
 - Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.

- Does the contingency plan address issues relative to pre-planned alternate locations? The contingency plan *shall* address any potential issues relative to pre-planned alternate locations. These include:
 - o insurance
 - o equipment replacement
 - o phones
 - o utilities
 - o security
- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities *shall* include:
 - o prioritizing operations
 - o identifying key personnel and how to reach them
 - o listing backup systems and where they are located
 - o stocking critical forms, blank check stock, and supplies off-site
 - developing reliable sources for replacing equipment on an emergency basis
- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?
- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?
- Have temporary data storage sites and location of stored backups been identified?
- Is the frequency of file backup documented?
- Have the arrangements been made for ensuring continuing communications capabilities?
- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?
- Are system, application, and other key documentation maintained at the offsite location?
- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?
- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs. These are stored at off-site locations sufficiently distant from the

primary site so as not to be affected by the same emergency that would affect the primary site.

- Is the contingency plan stored off-site at alternate/backup locations? Copies of the contingency plan *shall* be stored at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the contingency plan that are stored in a private home *shall* be protected from inadvertent access.
- 9. Required Resources
 - Are the following resources for supporting critical operations defined and available for an emergency?
 - o Hardware
 - o Software
 - o Communications
 - o Data
 - o Documents
 - o Facilities
 - o People
 - o Supplies
 - o Basic essentials (water, food, shelter, transportation, etc.)
 - Does the contingency plan provide for backup personnel? As the contingency plan is implemented, it is necessary to have additional people available to support recovery operations. The contingency plan *shall* specify who these people are and when they would normally be called into action.

10. Training

- Are management and staff trained to respond to emergencies? Security training *shall* include modules for management and staff relative to their roles for handling emergency situations.
- 11. Testing the Contingency Plan
 - Is there a section in the contingency plan that addresses testing of the plan?
 - Testing of the contingency plan *shall* address the following topics:
 - o Test Philosophy
 - o Test Plans
 - o Boundaries
 - o Live vs. Walkthrough vs. End-to-End Testing
 - o Test Reports
 - Responsibilities
- 12. Contingency Plan Maintenance

- Schedule
 - Is the contingency plan annually reviewed and tested? The contingency plan *shall* be reviewed and tested annually under conditions as close to an emergency as can be reasonably and economically simulated.
 - Is there a provision for updating the contingency plan annually?
 - o Is the contingency plan revised after testing, depending on test results?
- 13. Relationships/Interfaces
 - Does the contingency plan identify critical interfaces? Interfaces required to continue critical business functions should be identified. Refer to the System Security Plans.
 - Which outside (vendors, providers, banks, utilities, services, CMS) interfaces must be considered?
 - Is the plan compatible with plans of interacting organizations and systems?
 - What internal interfaces must be considered?
 - Is the plan compatible with plans of interacting organizations and systems?
 - Which corporate interfaces must be considered?
 - Are there special interfaces with corporate systems that must be addressed in the contingency plan?
- 14. Attachments

Does the contingency plan contain appropriate attachments, as listed below?

A. Actions for Each Phase

Are the actions to be taken in each phase (respond, recover, restore) of the contingency clearly described and related to organizations and/or people?

- B. Procedures
 - Are there detailed instructions for:
 - responding to emergencies?
 - o recovering?
 - restoring operations?

- Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency *shall* be in place.
- Are there procedures for addressing the situation where the processing site is intact, but people can't get to it because of a natural disaster? Can the business be operated remotely?
- Is there an implementation plan for working from home?
- C. Call Trees

Are there call lists with names, addresses, and phone numbers with priority order relative to whom to call first?

D. Hardware Inventory

Are there lists of all the hardware covered by the contingency plan?

E. Software Inventory

Are there lists of all the software covered by the contingency plan?

F. System Descriptions

Are all the systems covered by the contingency plan defined, including appropriate diagrams?

G. Alternate/Backup Site Information

Is there sufficient detail to completely describe the alternate and/or backup sites, including addresses, phone numbers, contacts, resources available at the sites, and, resources needed to be brought to the site?

H. Assets/Resources

Are there lists of all the needed resources for responding, recovery, and restoring operations?

I. Risk Assessment Summary

Has there been a realistic assessment of the nature and size of the possible threat and of the resources most at risk?

J. Agreements/Memo of Understanding

Are there agreements in place relative to the use of alternate/backup sites, special resources, outside suppliers, extra people, alternate communications, etc?

K. Manual Operations

Are manual operating procedures in place so that certain functions can continue manually if automated support is not available soon enough?

Manual processing procedures *shall* exist in the backup phase until automated capabilities can take over the information processing. Provisions *shall* be made to provide this manual capability.

L. Supplies/Materials/Equipment

Is there information that describes how and where to obtain needed supplies, materials, and equipment?

M. Floor Plans

Are the necessary floor plans available?

N. Maps

Are the necessary area and street maps available?

12 References

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

In addition to this manual, the following documents may be referenced during the IT systems contingency planning process:

- NIST Special Pub 800-34, Contingency Planning Guide for Information Technology Systems, June 2002. <u>http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf</u>
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 11. <u>http://csrc.nist.gov/publications/nistpubs/800-12</u>
- Health Insurance Portability & Accountability Act (HIPAA): The Race to Become Compliant, Ed Deveau, Disaster Recovery Journal, Fall 2000. http://hipaa.ascensionhealth.org/infoexchange/disaster.html
- Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6, Section 3.6.

http://www.gao.gov/special.pubs/12_19_6.pdf

- Presidential Decision Directive/NSC 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998. http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004. <u>http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html</u>
- Office of Management & Budget, Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, 8 February 1996. <u>http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html</u>
- CMS Contingency Planning Tabletop Test Procedures, Version 1.1., 25 July 2007. <u>http://www.cms.hhs.gov/informationsecurity/downloads/cp_tabletop_template.zip</u>

Appendix D: CMS Information Security (*IS*) Guidebook for Audits

1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This guide has been developed to aid contractors in understanding and preparing for the various types of audits and reviews, which may be performed at their locations. Its purpose is to provide additional information on site selection criteria, audit steps and objectives, documentation requirements, the types of employees that will need to be interviewed, space and equipment requirements for *Chief Financial Officer* (CFO)/*Electronic Data Processing (EDP)* audits, Section 912 Reviews, *Statement on Auditing Standards* (SAS) *No.* 70 type II audits, and Penetration/*External Vulnerability Assessment* (EVA) testing.

1.1 CFO/EDP Audits

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The purpose of these audits is to ensure that proper *information technology* (IT) controls exist within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IT controls is needed from each contractor site to determine the sufficiency of overall controls for Centers for Medicare & Medicaid Services (CMS). The level of controls is used to assess the impact of their presence on the financial statements and operations of CMS.

The Chief Financial Officer's Act of 1990 was enacted to improve the general and financial management of the Federal government and established the foundation for the Government Performance Results Act (GPRA). A CFO Act audit is conducted under the guidelines and supervision of the U.S. General Accountability Office (GAO). The GAO requires that all such audits follow the Federal Information Systems Control and Audit Manual (FISCAM). FISCAM includes 6 major areas: Entity-wide Security Program, Access Controls, Application Development and Change Control, Systems Software, Service Continuity, and Segregation of Duties.

1.2 Section 912 Evaluation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

As part of the Medicare Prescription Drug, Improvement and Modernization Act (MMA) of 2003, a requirement exists to perform an evaluation of the information security *(IS)* programs at the Medicare Fiscal Intermediaries and Carriers. The programs at these contractors *shall* be in compliance with the eight statutory requirements *(see below)* set forth in the Federal Information Security Management Act (FISMA).

These evaluations are conducted according to procedures established by the Office of Information Services (OIS) with input from the U.S. Department of Health and Human

Services (*DHHS*), Office of Inspector General (OIG). The procedures are organized using the eight FISMA statutory areas which include:

- 1. Periodic Information Security (IS) Risk Assessments (RA);
- 2. *P*olicies and procedures based on *IS RAs* that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the Systems Development Life Cycle (SDLC) and complies with the National Institute of Standards and Technology (NIST) standards;
- 3. System Security Plans (SSP);
- 4. Security awareness training;
- 5. *P*eriodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities;
- 6. *R*emedial activities, processes and reporting for deficiencies;
- 7. Incident detection, reporting and response; and
- 8. Continuity of operations for IT systems.

1.4 Penetration/EVA

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the GAO's FISCAM dated January 1999. The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal *government* domain.

A network vulnerability assessment is the systematic examination of an information system to:

- *D*etermine the adequacy of security measures,
- *I*dentify security deficiencies,
- *P*rovide data from which to predict the effectiveness of proposed security measures, and
- *C*onfirm the adequacy of such measures after implementation.

Penetration testing utilizes selected intrusion techniques that may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

2.1 CFO/EDP Audit Acts

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The purpose of these audits is to ensure that proper IT controls exist within each contractor, maintainer, or data center that supports Medicare processing. The assurance of IT controls is needed from each contractor site to determine the sufficiency of overall controls for CMS. The level of controls is used to assess the impact of their presence on the financial statements and operations of CMS.

A CFO Act audit is conducted under the guidelines and supervision of the U.S. GAO. The GAO requires that all such audits follow FISCAM. FISCAM includes 6 major areas: Entity-wide Security Program, Access Controls, Application Development and Change Control, Systems Software, Service Continuity, and Segregation of Duties.

One overall report is created for each site audited with the final report being issued by the OIG.

2.1.1 Site Selection Criteria

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Selection of sites to be included in the CFO Act *a*udit is primarily based on the volume of claims processed, prior findings, and significance of processing done. Smaller sites are rotated into the testing to ensure that their controls are also understood, but such sites are not likely to be audited every year. Because of the new requirements of the security evaluations set forth in Section 912 of the MMA (see section 2.2 of this guide for more detail), the need to rotate smaller sites into testing samples may diminish in the future.

2.1.2 Audit Steps and Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The *DHHS* OIG performs audit work on the following areas of FISCAM during their audits:

Physical Access Controls

- AC-1 Classify information resources according to their criticality and sensitivity.
 - o AC-1.1 Resource classifications and related criteria have been established.
 - o AC-1.2 Owners have classified resources.
- AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
 - AC-3.1 Adequate physical security controls have been implemented.
 - AC-3.1.A Physical safeguards have been established that are commensurate with the risks of physical damage or access.
 - AC-3.1.B Visitors are controlled.
 - AC-3.4 *Sanitation of equipment and media prior to disposal or reuse.*

Service Continuity

- SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.
 - SC-1.1 Critical data and operations are identified and prioritized.
 - SC-1.2 Resources supporting critical operations are identified.
 - SC-1.3 Emergency processing priorities are established.

- SC-2 Take steps to prevent and minimize potential damage and interruption.
 - SC-2.1 Data and program backup procedures have been implemented.
 - o SC-2.2 Adequate environmental controls have been implemented.
 - SC-2.3 Staff has been trained to respond to emergencies.
 - SC-2.4 Effective hardware maintenance, problem management, and change management *help* prevent unexpected interruptions.
- SC-3 Develop and document a comprehensive contingency plan.
 - SC-3.1 An up-to-date contingency plan is documented.
 - SC-3.2 Arrangements have been made for alternate data processing and telecommunications facilities.
- SC-4 Periodically test the contingency plan and adjust it as appropriate.
 - SC-4.1 The plan is periodically tested.
 - SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly.

The CMS-contracted auditor performs audit work on the following areas of FISCAM as part of the CFO Act audits:

Access Controls

- AC-2 Maintain a current list of authorized users and their access authorized.
 - AC-2.1 Resource owners have identified authorized users and their access authorized.
 - o AC-2.2 Emergency and temporary access authorization is controlled.
 - o AC-2.3 Owners determine disposition and sharing of data.
- AC-3 Establish physical and logical controls to prevent or detect unauthorized access.
 - AC-3.2 Adequate logical access controls have been implemented. (see also EVA)
 - AC-3.2.A Passwords, tokens, or other devices are used to identify and authenticate users.
 - AC-3.2.B Identification of access paths.
 - AC-3.2.C Logical controls over data files and software programs.
 - AC-3.2.D Logical control over *a* database.
 - AC-3.2.E Logical controls over telecommunications access.
 - AC-3.3 Cryptographic tools. (see also EVA)
- AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.
 - AC-4.1 Audit trails are maintained.
 - AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.

• AC-4.3 Suspicious access activity is investigated and appropriate action is taken.

2.1.4 Documentation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Documentation needed by the OIG for a CFO Act *audit* usually depends on the contractor's role in the Medicare system. This documentation includes, but is not limited to the following:

- 1. Entity-wide security programs (e.g., *SSP*)
- 2. Network diagrams
- 3. IS RAs and vulnerability analyses
- 4. Organizational charts which include names and titles for the Medicare, information systems, and information system security departments
- 5. *FISMA Evaluation* with Core Set of Security Requirements (*CSR*) using the CMS Integrated Security Suite (CISS)
- 6. *IS RA* policies and any internal risk analysis documentation
- 7. Documentation on data and resource classification
- 8. *Human Resource* (HR) policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
- 9. The most recent SAS 70 and *IS RA* reports
- 10. Policies and procedures regarding conduct in the data center
- 11. Policies and procedures for back-up tape rotation and off-site storage
- 12. Policies and procedures for sanitation of media prior to disposal
- 13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms
- 14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas
- 15. Layout of company buildings and overview of operations in each building

- 16. Employee lists for Medicare, information systems, and information system security departments (lists *shall* include: name or identification (ID) number, job title, department, start date, and position effective date)
- 17. Documentation of new hire information system security training program
- 18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas
- 19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract
- 20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests
- 21. Policies and procedures regarding the testing of the disaster recovery plan
- 22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable
- 23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan

Documentation needed by the CMS-contracted auditor for a CFO Act *audit* usually depends on the contractor's role in the Medicare system. This documentation includes, but is not limited to the following:

Application Development and Change Management

Information on change management, including the following:

- 1. SDLC methodology document
- 2. A list of all changes made during the current fiscal year
- 3. Dates of and training materials from the most recent SDLC training class
- 4. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)
- 5. A list of all authorized change request approvers
- 6. Policies and procedures over the use of personal and public domain software
- 7. Test plan standards

- 8. A log of *abends*
- 9. Procedures for new software distribution
- 10. Policies and procedures for emergency changes
- 11. A list of all emergency changes during the current fiscal year
- 12. Identification of virus software in use
- 13. A list of all users with access to library management software
- 14. A list of all users with access to the production libraries (production code, source code, extra program copies)
- 15. Tape library logs for the most recent 3 months

2.1.5 Interviews Required

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

- 1. Medicare compliance officer
- 2. Person responsible for the Corrective Action Plan (CAP)
- 3. Person responsible for *IS RA*
- 4. Person responsible for the *SSP*
- 5. Person in charge of training (entity wide security program)
- 6. Internal audit lead
- 7. HR contact
- 8. Mainframe systems administrator
- 9. Mainframe security administrator
- 10. Local Area Network (LAN) administrator
- 11. Network (LAN) security officer

- 12. Security software administrator
- 13. Systems programming manager
- 14. Person in charge of maintaining the System and Business Continuity Plan
- 15. Person in charge of the data center
- 16. Manager of physical security
- 17. Head of computer operations
- 18. Person in charge of change management
- 19. Application manager for the following systems:
 - a. Fiscal Intermediary Standard System (FISS)
 - b. MultiCarrier System/Mandatory Claim Submission System (MCS)
 - c. VIPS Medicare System (VMS)

2.2 Section 912 Evaluation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

As part of the MMA, a requirement exists to perform an evaluation of the *IS* programs at the Medicare Fiscal Intermediaries and Carriers. The programs at these contractors *shall* be in compliance with the eight statutory requirements set forth in the Federal Information Security Management Act (FISMA).

The CMS-contracted auditor has agreed to perform procedures established by CMS and the *DHHS* OIG associated with the eight FISMA statutory areas which include:

- 1. Periodic IS RAs;
- 2. Policies and procedures based on *IS RA*s that cost-effectively reduce risk to an acceptable level and ensure that security is addressed within the systems development life cycle and complies with the NIST standards;
- 3. System Security Plans;
- 4. Security awareness training;
- 5. Periodic testing and evaluation of the effectiveness of IT security policies and procedures, including network assessments and penetration activities;
- 6. Remedial activities, processes and reporting for deficiencies;
- 7. Incident detection, reporting and response; and
- 8. Continuity of operations for IT systems.

2.2.2 Audit Steps and Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Risk Assessments

- 1. Determine if the current system configuration is documented, including links to other systems.
- 2. Determine if *IS RA*s are performed and documented on an annual basis or whenever the system, facilities, or other conditions change.
- 3. Determine if data sensitivity and integrity of the data have been documented and if data have been classified.
- 4. Determine if threat sources, both natural and manmade, have been formally identified.
- 5. Determine if a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources has been developed and maintained current.
- 6. Determine if an analysis has been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities.
- 7. Determine if final risk determinations and related management approvals have been documented and maintained on file.
- 8. Determine if a mission/business impact analysis have been conducted and documented.
- 9. Obtain management's list of additional controls that have been identified to mitigate identified risks.

Policies and Procedures to Reduce Risk

- 1. Read the policies and procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in the *IS RA*s section above.
- 2. Determine if management activities include security controls in the costs of developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.
- 3. Determine if management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.
- 4. Determine the number of systems for which security controls have been tested and evaluated. Determine if the system/network boundaries have been subjected to periodic reviews/audits.

- 5. Read the results of management's compliance checklist with the CMS CSR to determine gaps in compliance.
- 6. Determine if security policies and procedures include controls to address platform security configurations and patch management.

Review of System Security Plans

- 1. Determine if a security plan is documented and approved.
- 2. Determine if the plan is kept current.
- 3. Determine if a security management structure has been established.
- 4. Determine if *IS* responsibilities are clearly assigned.
- 5. Determine if owners and users are aware of security policies.
- 6. Determine if security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications
- 7. Determine if hiring, transfer, termination, and performance policies address security.
- 8. Determine if employee background checks are performed.
- 9. Determine if security employees have adequate security training and expertise.
- 10. Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.
- 11. Determine if management ensures that corrective actions are effectively implemented.

Review of Security Awareness Training

- 1. Determine if employees have received a copy of the Rules of Behavior (*ROB*).
- 2. Determine if employee training and professional development has been documented and formally monitored.
- 3. Determine if there is mandatory annual refresher training for security.

- 4. Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.
- 5. Determine if employees have received a copy of or have easy access to agency security procedures and policies.
- 6. Determine if security professionals have received specific training for their job responsibilities, and if the type and frequency of application-specific training provided to employees and contractor personnel is documented and tracked.

Review of Periodic Testing and Evaluation of the Effectiveness of IT Security Policies

- 1. Determine if management reports exist for the review and testing of IT security policies and procedures, including network *IS RA*, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments.
- 2. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls).
- 3. Determine if remedial action is being taken for issues noted on audits.

Policies and Procedures for Continuity of Operations and Related Physical Security Safeguards for IT Systems.

- 1. Determine if critical data and operations are formally identified and prioritized.
- 2. Determine if resources supporting critical operations are identified in contingency plans.
- 3. Determine if emergency processing priorities are established.
- 4. Determine if data and program backup procedures have been implemented.
- 5. Determine if adequate environmental controls have been implemented.
- 6. Determine if staff has been trained to respond to emergencies.
- 7. Determine that hardware maintenance, problem management, and change management procedures exist to help prevent unexpected interruptions.
- 8. Determine if policies and procedures for disposal of data and equipment exist and include applicable *Federal* security and privacy requirements.

- 9. Determine if an up-to-date contingency plan is documented.
- 10. Determine if arrangements have been made for alternate data processing and telecommunications facilities.
- 11. Determine if the contingency plan is periodically tested.
- 12. Determine if the results are analyzed and the contingency plans are adjusted accordingly.
- 13. Determine if physical security controls exist to protect IT resources.

2.2.4 Documentation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Documentation needed for Section 912 includes but is not limited to the following areas:

Risk Assessment Review

- 1. Current system configurations documentation including links to other systems
- 2. *IS RA*s
- 3. Data classification policies/procedures
- 4. Threat source documentation (manmade/natural)
- 5. Documented system vulnerabilities, system flaws, or weaknesses
- 6. Risk determinations (assessments) with related management approvals
- 7. Mission/business impact analysis

System Security Plan

- 1. *SSP*
- 2. Security management structure
- 3. IS job responsibilities
- 4. Hiring, termination, transfer policies/procedures
- 5. Background check policies/procedures

- 6. Security policy/procedure updates
- 7. Management review of corrective actions

2.2.5 Interviews Required

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

- 1. Medicare compliance officer
- 2. Person responsible for the CAP
- 3. Person responsible for IS RA
- 4. Person responsible for the *SSP*
- 5. Person in charge of training (entity wide security program)
- 6. Internal audit lead
- 7. HR contact
- 8. Mainframe systems administrator
- 9. Mainframe security administrator
- 10. LAN administrator
- 11. LAN security officer
- 12. Security software administrator
- 13. Systems programming manager
- 14. Person in charge of maintaining the System and Business Continuity Plan
- 15. Person in charge of the data center
- 16. Manager of physical security
- 17. Head of computer operations
- 18. Person in charge of change management

- 19. Application manager for the following systems:
 - a. FISS
 - b. MCS
 - c. VMS

2.3 SAS 70 Audits

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

SAS 70, is an internationally recognized auditing standard developed by the AICPA. A SAS 70 audit or service auditor's examination is widely recognized because it indicates that a service organization has been through an in-depth audit of IT control activities and related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting firm. A formal report including the auditor's opinion (Service Auditor's Report) is issued to the service organization at the conclusion of a SAS 70 Audit.

2.3.2 Audit Steps and Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The planned focus of the audit team is collecting information through inquiry, inspection, and observation.

The CMS-contracted auditor will assess the effectiveness of the controls in place as *represented* by management's description of controls. Management's control objectives should be aligned with key FISCAM areas. These key areas include:

- Entity-wide Security Program
- Access Controls
- Control of Application Development and Implementation
- Systems Software
- Service Continuity
- Segregation of Duties

Typically the CMS-contracted auditor will assess the following (and other) control activities; contingent upon them being listed in management's description of controls:

A.1 An entity-wide security program has been documented, approved, and monitored by management in accordance with the CMS Business Partners Systems Security Manual (BPSSM) and includes requirements to assess security risks periodically, establish a security management structure, clearly assign security responsibilities, implement effective security-related personnel policies, monitor the security program's effectiveness, and ensure security officer training and employee security awareness.

- A.2 Security related personnel policies are implemented that include performance of background investigations and contacting references, include confidentiality agreements with employees (regular, contractual, and temporary) and include termination and transfer procedures that require exit interviews, return of property (such as keys and ID cards), notification to security management of terminations, removal of access to systems, and escorting of terminated employees out of the facility.
- A.3 Information resources are classified (risk-ranked) according to their criticality/sensitivity and are periodically formally reviewed.
- A.4 Access to computerized applications, systems software, and Medicare data are appropriately authorized, documented and monitored, includes approval by resource owners, procedures to control emergency and temporary access and procedures to share and properly dispose of data.
- A.5 Security policies and procedures include controls to ensure the security of platform configurations and to ensure proper patch management of operating systems.
- A.6 Physical access by all employees (including visitors) to Medicare facilities, data centers, and systems is appropriately authorized, documented, and access violations are monitored and investigated.
- A.7 Medicare application and related systems software development and maintenance activities are authorized, documented, tested, and approved.
- A.8 A *SDLC* methodology is documented and in use and includes planning for and costs for security requirements in systems.
- A.9 Change management policies and procedures exist that include documented testing and approval of changes for regular and emergency changes and restrictions on the use of public domain and personal software.
- A.10 Access to program libraries is properly restricted, and movement of programs among libraries is controlled.
- A.11 Adequate segregation of duties exists between various functions within Medicare operations and is supported by appropriately authorized and documented policies.
- A.12 Activities of employees *shall* be controlled via formal operating procedures that include monitoring of employee activities by management with

documentation maintained to provide evidence of management's monitoring and review process.

- A.13 A regular *IS RA* of the criticality and sensitivity of computer operations, including all network components, IT platforms and critical applications has been established and updated annually. The assessment includes identification of threats, known system vulnerabilities, system flaws, or weaknesses that could be exploited by threat sources.
- A.14 A centralized risk management focal point for I*S RA* has been established that includes promotion awareness programs, processes and procedures to mitigate risks and monitoring processes to assess the effectiveness of risk mitigation programs.
- A.15 An *IS RA* and *SSP* has been documented, approved, and monitored by management in accordance with the CMS *Information Security (IS)* Risk Assessment (*RA*) and Systems Security Plan (*SSP*) *Procedures*.
- A.16 Regularly scheduled processes required to support the Medicare contractor's continuity of operations (data, facilities or equipment) are performed.
- A.17 A corrective action management process is in place that includes planning, implementing, evaluating, and fully documenting remedial actions addressing findings noted from all security audits and reviews of IT systems, components and operations.
- A.18 Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.
- A.19 Management procedures are in place to ensure proper action in response to unusual activity, intrusion attempts, and actual intrusions.
- A.20 Management processes and procedures include reporting of intrusions attempts and intrusions in accordance with FISMA.

2.3.4 Documentation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Documentation needed for SAS 70 is specific to the control activities defined by management at each contractor site but may include the following:

- 1. Entity wide security programs (e.g., *SSP*)
- 2. Network diagrams
- 3. *IS RAs* and vulnerability analyses

- 4. Organizational charts that include names and titles for the Medicare, information systems, and information system security departments
- 5. Completed CSRs using the CISS
- 6. IS RA policies and any internal risk analysis documentation
- 7. Documentation on data and resource classification
- 8. HR policies and procedures regarding hiring, transfers, terminations, confidentiality agreements, vacations, and job rotations
- 9. The most recent SAS 70 and *IS RA* reports
- 10. Policies and procedures regarding conduct in the data center
- 11. Policies and procedures for back-up tape rotation and off-site storage
- 12. Policies and procedures for sanitation of media prior to disposal
- 13. Policies and procedures for physical access for normal operations and emergency situations with applicable authorization forms
- 14. Policies and procedures regarding visitors to both the general campus and to the sensitive areas
- 15. Layout of company buildings and overview of operations in each building
- 16. Employee lists for Medicare, information systems, and information system security departments (lists *shall* include: name or identification (ID) #, job title, department, start date, and position effective date)
- 17. Documentation of new hire/information system security training program
- 18. Vendor sign in and sign out logs for maintenance or repairs in sensitive areas
- 19. Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract
- 20. Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests
- 21. Policies and procedures regarding the testing of the plan

- 22. Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable
- 23. Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity-wide security plan
- 24. Security policies, standards, and procedures for:
 - a. Creation, modification, and deletion of user-IDs, functional groups, etc.
 - b. Periodic review of access
 - c. Dial-up access
 - d. Use and monitoring of emergency or temporary access (Fire-call IDs)
 - e. Password composition/mask
 - f. Violation and security monitoring
 - g. Archiving, deleting, or sharing data files
 - h. Monitoring of critical security software reports (For RACF DSMON, SETROPTS, etc.)
- 25. List of all terminations during the current fiscal year
- 26. List of all transfers during the current fiscal year
- 27. List of all new hires during the current fiscal year
- 28. List of all Medicare application users
- 29. List of all users with dial up access
- 30. List of all users with the ability to change security settings (administrators)
- 31. Access to access requests and authorizations (for a sample of users)
- 32. List of access request approvers
- 33. Documentation supporting recertification of users
- 34. List of emergency or temporary (fire-call) IDs
- 35. Activity log of emergency or temporary IDs
- 36. Contracts/confidentiality clauses with vendor(s) if data is being shared with other parties
- 37. System default password requirements
- 38. Use of generic, group or system IDs

- 39. Database security requirements and settings
- 40. Security violation logging and monitoring
- 41. Evidence of review of user templates and/or profiles
- 42. Evidence of automatic timeout on terminals
- 43. Database access lists
- 44. Evidence supporting resolution of prior year audit findings
- 45. Results of CA_EXAMINE runs
- 46. Policies and procedures for restricting access to systems software
- 47. A list of all system programmers
- 48. A list of all application programmers
- 49. A list of all computer operators
- 50. Results of the last review of system programmer access capabilities
- 51. A list of all vendor supplied software indicating the current version of the software
- 52. If available, integrity statements from vendors for all third party software
- 53. Policies and procedures for using and monitoring use of system utilities
- 54. Policies and procedures for identifying, selecting, installing and modifying systems software
- 55. Policies and procedures for disabling vender supplied defaults
- 56. Roles and responsibilities for system programmers
- 57. Policies and procedures for emergency software changes
- 58. A list of all systems software changes made during the fiscal year
- 59. A list of all emergency changes made during the fiscal year
- 60. A list of all current access to systems software

- 61. A list of all users with access to migrate programs to production
- 62. A sample of audit logs for system utilities and system programmer activity
- 63. Evidence of review of logs and follow up action taken
- 64. IPL procedures
- 65. Log from last IPL
- 66. SDLC methodology document
- 67. Change control policies and procedures (if not included in the SDLC document)
- 68. A list of all changes made during the current fiscal year
- 69. Dates of and training materials from the most recent SDLC training class
- 70. Implementation requests/orders for all changes made during the current fiscal year (a specific sample will be drawn during fieldwork)
- 71. A list of all authorized change request approvers
- 72. Policies and procedures over the use of personal and public domain software:
- 73. Test plan standards
- 74. A log of abends
- 75. Procedures for new software distribution
- 76. Policies and procedures for emergency changes
- 77. A list of all emergency changes during the current fiscal year
- 78. Identification of virus software in use
- 79. A list of all users with access to library management software
- 80. A list of all users with access to the production libraries (production code, source code, extra program copies)
- 81. Tape library logs for the most recent 3 months
- 82. Current system configurations documentation including links to other systems

- 83. Threat source documentation (manmade/natural)
- 84. Documented system vulnerabilities, system flaws or weaknesses
- 85. Mission/business impact analysis
- 86. Job descriptions for management
- 87. IS job responsibilities
- 88. Background check policies/procedures
- 89. Security policy/procedure updates
- 90. Management review of corrective actions
- 91. Training/professional development policies/procedures
- 92. Training schedule (if applicable)
- 93. Awareness posters, booklets, newsletters, etc
- 94. Management reports for review & testing of IT security policies & procedures
- 95. Independent audit reports and evaluations
- 96. Tracking of weaknesses (DB, paper, etc)
- 97. Planned corrective actions
- 98. CAP
- 99. List of IT security weaknesses including dates of corrective actions
- 100. Policies/procedures for monitoring systems & the network
- 101. Policies/procedures for management response to unusual activity, intrusion attempts and actual intrusions

2.3.5 Interviews Required

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The CMS-contracted auditor shall interview the following Medicare contractor employees:

- 1. Medicare compliance officer
- 2. Person responsible for the CAP
- 3. Person responsible for IS RA
- 4. Person responsible for the *SSP*
- 5. Person in charge of training (entity wide security program)
- 6. Internal audit lead
- 7. HR contact
- 8. Mainframe systems administrator
- 9. Mainframe security administrator
- 10. LAN administrator
- 11. LAN security officer
- 12. Security software administrator
- 13. Systems programming manager
- 14. Person in charge of maintaining the System and Business Continuity Plan
- 15. Person in charge of the data center
- 16. Manager of physical security
- 17. Head of computer operations
- 18. Person in charge of change management
- 19. Application manager for the following systems:
 - a. FISS
 - b. MCS
 - c. VMS

2.4 Penetration/EVA

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Network vulnerability assessments and penetration testing of information systems are required under the Access Controls domain of the GAO FISCAM, dated January 1999.

The Rules of Engagement section of FISCAM establishes guidelines to assist the execution of network vulnerability assessments and penetration testing in the Federal *government* domain.

For purposes of this engagement, a network vulnerability assessment is the systematic examination of an information system, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Penetration testing utilizes selected intrusion techniques that may be used by an actual intruder to compromise network security. Penetration testing also evaluates the effectiveness of an organization's security incident response capability.

2.4.1 Execution of the Audit

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Due to the sensitive nature of the testing, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results. The testing includes procedures to demonstrate both external and internal threats. To ensure that the integrity of the testing is not impaired, parties with knowledge of the testing are requested to restrict communicating any aspects, including test schedules to individuals at the operational level prior to or during test performance.

The CMS-contracted auditor is the Independent Public Accountant (IPA) engaged by the *DHHS* OIG to perform testing at third party CMS contractors as part of the FY 2004 Financial Statement Audit of CMS. There will be a site summary that includes a high level description of the testing performed and findings describing technical issues identified during testing. The findings will be written in terms of Condition, Cause, Criteria, Effect, and Recommendation (following GAO Yellow Book guidelines). The Site Summary will be supported by summary work papers for each type of testing performed.

2.4.3 Audit Steps and Objectives

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Steps to Perform Penetration Testing

Phase 1 – Assess & Model Threats

The Assess & Model Threats phase is used to establish and acquire the information required to successfully define the scope of the security penetration testing. This involves gathering information and completing an initial threat analysis to ensure that testing emulates the threats that are of real concern to the organization. This includes project start-up, information gathering and threat analysis.

- 1. Threat analysis is usually conducted according to prescribed scenarios that are clearly documented in the Statement of Work. Some common threat scenarios for an external penetration test include:
 - a. **Untrusted Outsider** This is the most common scenario for an External (Internet) penetration test. This scenario is designed to simulate individuals with no significant knowledge of the client's computing operations that are attempting to gain access from remote locations;
 - b. **Trusted Outsider** This scenario is designed to simulate third parties (e.g., customers, suppliers, partners) that have limited legitimate access to the client's network. In the event of the trusted outsider scenario, establish with the client what resources the team will attack and arrange for the client to set up valid credentials to access those resources (e.g., usernames/passwords, SecurID tokens).
- 2. During the project start-up, agree on primary contacts for both the CMScontracted auditor and the client to contact in case of an emergency. These contact numbers *shall* be accessible at all times during testing. All members of the team should be aware of the escalation path and procedures during testing.
- 3. Determine with the client when testing should stop. Some clients request that as soon as access is obtained, the CMS-contracted auditor stop and notify the client before attempting to obtain further access to resources.
- 4. Determine if there are specific targets of interest that the CMS-contracted auditor should direct attacks to (e.g., a focus on the client's web server).
- 5. All penetration activities *shall* be conducted from either a CMS-contracted auditor lab or the client site. Identify the source *Internet Protocol* (IP) range you will be using with the client to allow them to differentiate the CMS-contracted auditor activities from legitimate hacking attempts. Contact your lab manager for information on your external IP address range.
- 6. Establish acceptable timeframes for penetration testing with the client to avoid disrupting day-to-day client business (and to avoid being caught if the engagement requires stealth testing).
- 7. Inquire about any IP addresses that should be excluded from testing.

Phase 2 – Survey Testing

The Survey Testing phase is used to identify and document client devices that may be accessed from the Internet and to determine if any of these devices might be vulnerable to well-known exploits. This includes gathering IP address, MAC address, operating

system, web server, application, and enticement information, in addition to any other salient information about the target environment.

- 1. Identify Internet connections and IP ranges by querying public databases.
- 2. Identify salient target information available in newsgroups and web pages.
- 3. Use DNS queries to identify client networks and systems. These queries are best performed from a UNIX system that has the dig utility installed (NOTE: *D*ig is also available for Windows systems). IP addresses that are found through DNS queries should be looked up in the Internet repositories listed above to determine the range and owner of the IP address. The following queries can be used to identify client systems and networks:
- 4. Once you have identified client IP ranges and accessible websites, confirm IP addresses with the client contact before attempting to attack any systems.
 - a. Once the client has approved the IP ranges identified during the first part of this phase, scans can be conducted using a map to identify open ports and potential attack points on each of the servers in the range. Depending on the requirements of the organization, different types of scans may be used to try and avoid detection.
- 5. Once the initial scan is complete, a table should be created for the information gathered from each port.
- 6. After you have identified the services running on each port and obtained all information possible, the Intrusion Testing Phase of the engagement can begin. Note: confirm with the engagement manager before beginning Intrusion testing to determine if the client needs to be notified before beginning.

Phase 3 – Intrusion Testing

The Intrusion Testing phase is used to examine the weaknesses found and, where appropriate, attempt to exploit these weaknesses to demonstrate the risks and exposures. This stage is the core of the security penetration test and may be an iterative process as one exploited weakness may give rise to further exploitation opportunities.

The overall goal of the Intrusion Testing phase is to demonstrate access to systems and the capability to exploit this access further, not necessarily to gain full uncontrolled access to systems, although there may be instances where such access may be permissible.

1. Each attempt you make to gain access to systems (including every username and password combination) *shall* be documented. There are an infinite number of

avenues to attempt to gain access to a system, but the intrusion attempts should be performed in the following order.

- 2. If you gain access to a system, take a screen shot and SLOW DOWN.
- 3. Navigate the filesystem and attempt to identify any sensitive data files. These may include usernames, passwords or SMTP strings.
- 4. Use the machine as a "stepping stone" and exploit any trust relationships to compromise additional machines. Determine any network interfaces this system has (e.g., network interface cards) and determine what capabilities the system gives you (e.g., ping internally, telnet). Further system testing, such as this, should be conducted according to the same procedures prescribed so far: (1) Assess and Model Threats; (2) Survey Testing; and (3) Intrusion Testing.

2.4.4 Documentation

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Documentation and other items needed for Penetration/EVA includes, but is not limited to:

- 1. Network Architecture diagrams and descriptions for the performance of internal diagnostic reviews.
- 2. Site / system password policies
- 3. Applicable phone number range for dial-up "war-dialing" testing.
- 4. Applicable IP address spaces for penetration testing.
- 5. Listing of IP addresses assigned to, or under the purview of the site.
- 6. Listing of prohibited telephones/systems/networks
- 7. Standards and Guidelines (Risk Model) for system configuration.

Additional Penetration/EVA Items include:

- 1. Personnel to observe the penetration and diagnostic testing activities (if desired by the auditee).
- 2. Permission to connect the CMS-contracted auditor laptop to site's network (while monitored).
- 3. Network access for internal testing.

System administrator/programmer access for systems to perform diagnostic review.

4. Specific documents required by the CMS-contracted auditor will be requested in the Provided by Client (PBC) list. This list will be provided prior to the start of testing.

3 Tables

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This table provides a synopsis of required documentation.

Documentation	CFO Audit	Section 912	SAS 70	EVA
Entity wide security programs (e.g., <i>SSP</i>)	~	~	~	
Network diagrams	~	~	~	~
IS RAs and vulnerability analyses	~	~	>	
Organizational charts which include names and titles	>	~	<	
for the Medicare, information systems, and				
information system security departments				
Completed CSRs using the CISS	~	~	>	
IS RA policies and any internal risk analysis	>	~	<	
documentation				
Documentation on data and resource classification	~	~	<	
HR policies and procedures regarding hiring,	~	~	~	
transfers, terminations, confidentiality agreements,				
vacations, and job rotations				
The most recent SAS 70 and <i>IS RA</i> reports	~		>	
Policies and procedures regarding conduct in the	~		<	
data center				
Policies and procedures for back-up tape rotation	~	~	<	
and off-site storage				
Policies and procedures for sanitation of media prior	~	~	<	
to disposal				
Policies and procedures for physical access for	~		>	
normal operations and emergency situations with				
applicable authorization forms				
Policies and procedures regarding visitors to both	~		~	
the general campus and to the sensitive areas				
Layout of company buildings and overview of	~		~	
operations in each building				

Table D-1. Synopsis of Documentation Required

Documentation	CFO Audit	Section 912	SAS 70	EVA
Employee lists for Medicare, information systems, and information system security departments (lists <i>shall</i> include: name or identification (ID) #, job		~	~	
title, department, start date, and position effective date)				
Documentation of new hire/information system security training program	~	~	>	
Vendor sign in and sign out logs for maintenance or repairs in sensitive areas	~		>	
Contracts for off-site tape storage and alternate processing facilities and description of the off-site tape storage facility if not included in the contract	~		~	
Copy of most recent disaster recovery plan and results from the previous two disaster recovery tests.	~	~	~	
Policies and procedures regarding the testing of the plan	~	~	~	
Policies and procedures regarding hardware maintenance and/or contracts with maintenance providers if applicable	~	~	~	
Documentation of fire and other emergency drills held within the past year and emergency procedures guide if different than, or not included in the entity- wide security plan	~	~	~	
Security policies, standards, and procedures for:				
• Creation, modification, and deletion of user- IDs, functional groups, etc.	~		•	
Periodic review of access	~		~	
• Dial-up access	~		~	
• Use and monitoring of emergency or temporary access (Fire-call IDs)	~		~	
Password composition/mask	~		~	~
• Violation and security monitoring	~		~	
• Archiving, deleting, or sharing data files	~		~	
• Monitoring of critical security software reports (For RACF - DSMON, SETROPTS, etc.)	~		~	
List of all terminations during the current fiscal year	~		~	
List of all transfers during the current fiscal year	~		~	
List of all new hires during the current fiscal year	>		~	
List of all Medicare application users/	>	~	~	
List of all users with dial up access	~		~	
List of all users with the ability to change security	~		~	
settings (administrators)				

Documentation	CFO Audit	Section 912	SAS 70	EVA
Access to access requests and authorizations (for a	~		~	
sample of users)				
List of access request approvers	~		~	
Documentation supporting recertification of users	~		~	
List of emergency or temporary (fire-call) IDs	~		~	
Activity log of emergency or temporary IDs	~		~	
Contracts/confidentiality clauses with vendor(s) if	~		~	
data is being shared with other parties				
System default password requirements	~		~	
Use of generic, group or system IDs	~		~	
Database security requirements and settings	~		~	
Security violation logging and monitoring	~		~	
Evidence of review of user templates and/or profiles	~		~	
Evidence of automatic timeout on terminals	~		~	
Database access lists	~		~	
Evidence supporting resolution of prior year audit	~		~	
findings				
Results of CA_EXAMINE runs	~		~	
Policies and procedures for restricting access to	~		~	
systems software				
A list of all system programmers	~		~	
A list of all application programmers	~		~	
A list of all computer operators	~		~	
Results of the last review of system programmer	~		~	
access capabilities				
A list of all vendor supplied software that indicates	~		~	
how current the software is				
If available, integrity statements from vendors for all	~		~	
third party software				
Policies and procedures for using and monitoring	~		~	
use of system utilities				
Policies and procedures for identifying, selecting,	~		~	
installing and modifying systems software				
Policies and procedures for disabling vender	~		~	
supplied defaults				
Roles and responsibilities for system programmers			~	~
Policies and procedures for emergency software	~		~	
changes				
A list of all systems software changes made during	~		~	
the fiscal year				
A list of all emergency changes made during the	~		~	
fiscal year				
A list of all current access to systems software	~		~	

Documentation	CFO Audit	Section 912	SAS 70	EVA
A list of all users with access to migrate programs to	~		~	
production				
A sample of audit logs for system utilities and	~		~	
system programmer activity				
Evidence of review of logs and follow up action	~		~	
taken				
IPL procedures	~		~	
Log from last IPL	~		~	
SDLC methodology document	~	✓	~	
Change control policies and procedures (if not	~		~	
included in the SDLC document)				
A list of all changes made during the current fiscal	~		~	
year				
Dates of and training materials from the most recent	~		~	
SDLC training class				
Implementation requests/orders for all changes made	~		~	
during the current fiscal year (a specific sample will				
be drawn during fieldwork)				
A list of all authorized change request approvers	~		~	
Policies and procedures over the use of personal and	~		~	
public domain software:				
Test plan standards	~		~	
A log of <i>abends</i>	~		~	
Procedures for new software distribution	~		~	
Policies and procedures for emergency changes	~		~	
A list of all emergency changes during the current	~		~	
fiscal year				
Identification of virus software in use	~		~	
A list of all users with access to library management	~		~	
software				
A list of all users with access to the production	~		~	
libraries (production code, source code, extra				
program copies)				
Tape library logs for the most recent 3 months	~		~	
Current system configurations documentation		~	~	
including links to other systems				
Threat source documentation (manmade/natural)		~	~	
Documented system vulnerabilities, system flaws or		✓	~	
weaknesses				
Mission/business impact analysis		~	~	
Job descriptions for management		~	~	
IS job responsibilities		~	~	
Background check policies/procedures		~	~	

Documentation	CFO Audit	Section 912	SAS 70	EVA
Security policy/procedure updates		~	~	
Management review of corrective actions		~	~	
Training/professional development		~	~	
policies/procedures				
Training schedule (if applicable)		~	~	
Awareness posters, booklets, newsletters, etc		~	~	
Management reports for review & testing of IT		~	~	
security policies & procedures				
Independent audit reports and evaluations		~	~	
Tracking of weaknesses (DB, paper, etc)		~	~	
Planned corrective actions		~	~	
All four quarter CAPs		~	~	
List of IT security weaknesses including dates of		~	~	
corrective actions				
Policies/procedures for monitoring systems & the		~	~	
network				
Policies/procedures for management response to		✓	~	
unusual activity, intrusion attempts and actual				
intrusions				
Network Architecture diagrams and descriptions for				✓
the performance of internal diagnostic reviews.				
Standards and Guidelines (Risk Model) for system				~
configuration.				
Applicable phone number range for dial-up "war-				~
dialing" testing.				
Applicable IP address spaces for penetration testing.				~
Listing of IP addresses assigned to, or under the				✓
purview of the site.				
Listing of prohibited telephones/systems/networks				✓

	etailed CFO Testing Procedures
Control Activity	Detailed Testing
Access Control	
	rces according to their criticality and sensitivity.
1. Resource classifications and	1. Review policies and procedures.
related criteria have been	2. Interview resource owners.
established.	
2. Owners have classified	1. Review resource classification documentation and
resources.	compare to <i>RA</i> s. Discuss any discrepancies with
	appropriate officials.
AC-3 Establish physical and logi	ical controls to prevent or detect unauthorized access.
1. Adequate physical security cont	rols have been implemented.
A. Physical safeguards have	1. Review a diagram of the physical layout of the
been established that are	computer, telecommunications, and cooling system
commensurate with the	facilities.
risks of physical damage or	2. Walk through facilities.
access.	3. Review risk analysis.
	4. Review lists of individuals authorized access to
	sensitive areas and determine the appropriateness
	for access.
	5. Before becoming recognized as the auditor, attempt
	to access sensitive areas without escort or
	identification badges.
	6. Observe entries to and exits from facilities during
	and after normal business hours.
	7. Observe utilities access paths.
	8. Interview management.
	9. Observe entries to and exits from sensitive areas
	during and after normal business hours.
	10. Interview employees.
	11. Review procedures for the removal and return of
	storage media from and to the library.
	12. Select from the log some returns and withdrawals,
	verify the physical existence of the tape or other
	media, and determine whether proper authorization
	was obtained for the movement.
	13. Observe practices for safeguarding keys and other
	devices.
	14. Review written emergency procedures.
	15. Examine documentation supporting prior fire drills
	16. Observe a fire drill.
B. Visitors are controlled.	1. Review visitor entry logs.
	2. Observe entries to and exits from sensitive areas
	during and after normal business hours.
	3. Interview guards at facility entry.

	ontrol Activity	De	tailed Testing
		4.	Review documentation on and logs of entry code
			changes.
		5.	Observe appointment and verification procedures
			for visitors.
2.	Sanitation of equipment and	1.	Review written procedures.
	media prior to disposal or	2.	Interview personnel responsible for clearing
	reuse.		equipment and media.
		3.	For a selection of recently discarded or transferred
			items, examine documentation related to clearing of
			data and software.
		4.	For selected items still in the entity's possession,
			test that they have been appropriately sanitized.
	ntity Wide Security Program		
	P-1 Risks are periodically asses	ssed	
1.	Risks are periodically assessed.	1.	Review <i>RA</i> policies.
		2.	Review the most recent high-level <i>RA</i> .
		3.	Review the objectivity of personnel who performed
			and reviewed the assessment.
SF	P-2 Document an entitywide se	curi	ty program plan.
1.	A security plan is documented	1.	Review the security plan.
	and approved.	2.	Determine whether the plan covers the topics
			prescribed by OMB Circular A-130.
2.	The plan is kept current.	1.	Review the security plan and any related
2.			
			documentation indicating that it has been reviewed
			documentation indicating that it has been reviewed and updated and is current.
SF		eme	-
SF	P-3 Establish a security manag responsibilities.	jeme	and updated and is current.
	responsibilities. A security management		and updated and is current.
	responsibilities.	1.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart.
	responsibilities. A security management	1. 2.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff.
	responsibilities. A security management	1. 2.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart.
	responsibilities. A security management	1. 2.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff.
	responsibilities. A security management	1. 2.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job
	responsibilities. A security management	1. 2. 3.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions.
1.	responsibilities. A security management structure has been established. IS responsibilities are clearly	1. 2. 3. 4.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions. Interview the security manager. Review the security plan.
1.	responsibilities. A security management structure has been established. IS responsibilities are clearly assigned.	1. 2. 3. 4. 1.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions. Interview the security manager. Review the security plan. Review documentation supporting or evaluating the
1.	responsibilities. A security management structure has been established. IS responsibilities are clearly assigned. Owners and users are aware of	1. 2. 3. 4. 1. 1.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions. Interview the security manager. Review the security plan.
1.	responsibilities. A security management structure has been established. IS responsibilities are clearly assigned. Owners and users are aware of	1. 2. 3. 4. 1. 1.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions. Interview the security manager. Review the security plan. Review documentation supporting or evaluating the awareness program. Observe a security briefing.
1.	responsibilities. A security management structure has been established. IS responsibilities are clearly assigned. Owners and users are aware of	1. 2. 3. 4. 1. 1.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions. Interview the security manager. Review the security plan. Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Determine
1.	responsibilities. A security management structure has been established. IS responsibilities are clearly assigned. Owners and users are aware of	1. 2. 3. 4. 1. 2.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions. Interview the security manager. Review the security plan. Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Determine what training they have received and if they are
1.	responsibilities. A security management structure has been established. IS responsibilities are clearly assigned. Owners and users are aware of	1. 2. 3. 4. 1. 2.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions. Interview the security manager. Review the security plan. Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities.
1.	responsibilities. A security management structure has been established. IS responsibilities are clearly assigned. Owners and users are aware of	1. 2. 3. 4. 1. 2. 3. 3.	and updated and is current. nt structure and clearly assign security Review the security plan and the entity's organization chart. Interview security management staff. Review pertinent organization charts and job descriptions. Interview the security manager. Review the security plan. Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities. Review memos, electronic mail files, or other

Control Activity	Detailed Testing
Control Activity	
	5. Call selected users, identify yourself as security or
	network staff, and attempt to talk them into
	revealing their password.
4. An incident response	1. Interview security manager, response team
capability has been	members, and system users.
implemented.	2. Review documentation supporting incident handling
	activities.
	3. Determine qualifications of response team
	members.
SP-4 Implement effective security	ty-related personnel policies.
1. Hiring, transfer, termination,	1. Review hiring policies.
and performance policies	2. For a selection of recent hires, inspect personnel
address security.	records and determine whether references have been
	contacted and background checks have been
	performed.
	3. Review reinvestigation policies.
	4. For a selection of sensitive positions, inspect
	personnel records and determine whether
	background reinvestigations have been performed.
	5. Review policies on confidentiality or security
	agreements.
	6. For a selection of such users, determine whether
	confidentiality or security agreements are on file.
	7. Review vacation policies.
	8. Inspect personnel records to identify individuals
	who have not taken vacation or sick leave in the
	past year.
	9. Determine who performed vacationing employee's
	work during vacation.
	10. Review job rotation policies.
	11. Review staff assignment records and determine
	whether job and shift rotations occur.
	12. Review pertinent policies and procedures.
	13. For a selection of terminated or transferred
	employees, examine documentation showing
	compliance with policies.
	14. Compare a system-generated list of users to a list of
	active employees obtained from personnel to
	determine if IDs and passwords for terminated
	employees exist.
2. Employees have adequate	1. Review job descriptions for security management
training and expertise.	personnel, and for a selection of other personnel.
und expertise.	Personner, and for a berechten of other personner.

Control ActivityDetailed Testing2. For a selection of employees, con	
\perp	nnara norgannal
records on education and experie	ence with job
descriptions.	
3. Review training program docume	
4. Review training records and related	
showing whether such records ar	
whether employees are receiving	the appropriate
training.	
SP-5 Monitor the security program's effectiveness and make change	es as needed.
1. Management periodically 1. Review the reports resulting from	n recent
assesses the appropriateness of assessments, including the most r	recent FMFIA
security policies and report.	
compliance with them. 2. Determine when the last indepen	dent review or
audit occurred and review the res	
3. Review written authorizations or	accreditation
statements.	
4. Review documentation related to	o corrective actions.
2. Management ensures that 1. Review the status of prior-year a	
corrective actions are recommendations and determine	
effectively implemented. corrective actions have been teste	
2. Review recent FMFIA reports.	
Segregation of Duties	
SD-1 Segregate incompatible duties and establish related policies.	
1. Incompatible duties have been 1. Review pertinent policies and process	ocedures
identified and policies 2. Interview selected management a	
	and 15 personner
	hart chowing IC
5. Review an ageney organization e	_
functions and assigned personnel	
4. Interview selected personnel and	
functions are appropriately segre	Ŭ
5. Determine whether the chart is cu	
function is staffed by different in	
6. Review relevant alternate or back	1 0
and determine whether the prope	r segregation of
duties is maintained.	
7. Observe activities of personnel to	
nature and extent of compliance	with the intended
segregation of duties.	
8. Review the organizational chart a	and interview
personnel to determine that assig	nments do not
result in a single person being res	sponsible for the
indicated combination of function	ns.

Control Activity	Detailed Testing
	10. Determine through interview and observation
	whether data processing personnel and security
	managers are prohibited from these activities.
	11. Review the adequacy of documented operating
	procedures for the data center.
2. Job descriptions have been	1. Review job descriptions for several positions in
documented.	organizational units and for user security
	administrators.
	2. Determine whether duties are clearly described and
	prohibited activities are addressed.
	3. Review the effective dates of the position
	descriptions and determine whether they are
	current.
	4. Compare these descriptions with the current
	responsibilities and duties of the incumbents in
	these positions to determine the accuracy of these
	statements.
	5. Review job descriptions and interview management
	personnel.
3. Employees understand their	1. Interview personnel filling positions for the selected
duties and responsibilities.	job descriptions (see above). Determine if the
	descriptions match their understanding of their duties and responsibilities and whether additional
	duties and responsibilities and whether additional duties are undertaken that are not listed in their job
	descriptions.
	2. Determine from interviewed personnel whether
	senior management has provided adequate
	resources and training to establish, enforce, and
	institutionalize the principles of segregation of
	duties.
	3. Interview management personnel in these activities.
SD-2 Establish access controls to	enforce segregation of duties.
1. Physical and logical access	1. Interview management and subordinate personnel.
controls have been established.	
2. Management reviews	1. Interview management and subordinate personnel.
effectiveness of control	2. Select documents or actions requiring supervisory
techniques.	review and approval for evidence of such
	performance (e.g., approval of input of transactions,
	software changes).
	3. Determine which reviews are conducted to assess
	the adequacy of duty segregation. Obtain and
	review the results of such reviews.
SD-3 Control personnel activitie supervision and review.	s through formal operating procedures and
Supervision and review. 1. Formal procedures guide	1. Review manuals.
1. Formar procedures guide	

Control Activity	Detailed Testing
personnel in performing their	2. Interview supervisors and personnel.
duties.	3. Observe processing activities.
2. Active supervision and review	1. Interview supervisors and personnel.
are provided for all personnel.	 Observe processing activities.
are provided for an personner.	 Review history log reports for signatures indicating
	supervisory review.
	4. Determine who is authorized to perform the <i>IPL</i> for
	the system, what steps are followed, and what
	controls are in place to monitor console activity
	during the process. Determine whether operators
	override the IPL parameters.
Service Continuity	
	ensitivity of computerized operations and identify
supporting resources.	
1. Critical data and operations are	1. Review related policies.
identified and prioritized.	2. Review list and any related documentation.
	3. Interview program, data processing, and security
	administration officials. Determine their input and
	their assessment of the reasonableness of priorities
	established.
2. Resources supporting critical	1. Review related documentation.
operations are identified.	2. Interview program and security administration
	officials.
3. Emergency processing	1. Review related policies.
priorities are established.	2. Review related documentation.
	3. Interview program and security administration
	officials.
	minimize potential damage and interruption.
1. Data and program backup	1. Review written policies and procedures for backing
procedures have been	up files.
implemented.	2. Compare inventory records with the files
	maintained off-site and determine the age of these
	files.
	3. For a selection of critical files, locate and examine
	the backup files. Verify that backup files can be
	used to recreate current reports.
	4. Determine whether backup files are created and
	rotated off-site as prescribed and are sent before
	prior versions are returned.5. Locate and examine documentation.
2 Adaquata anninan martal	6. Examine the backup storage site.
2. Adequate environmental controls have been	1. Examine the entity's facilities
controis nave been	2. Interview site managers.

Control Activity	Detailed Testing
Control Activity implemented.	 Detailed Testing Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shutoff valves, breathing apparatus, and other devices that they may be expected to use in an emergency. Observe the operation, location, maintenance and access to the air-cooling system. Observe whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor. Determine whether the activation of heat and smoke detectors will notify the fire department. Review documentation supporting recent tests of environmental controls. Review policies and procedures regarding employee behavior.
3. Staff has been trained to respond to emergencies.	 10. Observe employee behavior. 1. Interview data center staff. 2. Review training records. 3. Review training course documentation. 4. Review emergency response procedures. 5. Review test policies. 6. Review test documentation. 7. Interview data center staff.
4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	 Review policies and procedures. Interview data processing and user management. Review maintenance documentation. Interview data center management. Interview senior management, data processing management, and user management. Review supporting documentation.
SC-3 Develop and document a d	
 An up-to-date contingency plan is documented. 	 Review the contingency plan and compare its provisions with the most recent <i>RA</i> and with a current description of automated operations. Interview senior management, data center management, and program managers. Review the contingency plan. Interview senior management, data center management, and program managers. Observe copies of the contingency plan held off- site.

Control Activity	Detailed Testing		
	6. Review the plan and any documentation supporting		
	recent plan reassessments.		
2. Arrangements have been made	1. Review contracts and agreements.		
for alternate data processing			
and telecommunications			
facilities.			
SC-4 Periodically test the conting	gency plan and adjust it as appropriate.		
1. The plan is periodically tested.	1. Review policies on testing.		
	2. Review test results.		
	3. Observe a disaster recovery test.		
2. Test results are analyzed and	1. Review final test report.		
contingency plans are adjusted	2. Interview senior managers to determine if they are		
accordingly.	aware of the test results.		
	3. Review any documentation supporting contingency		
	plan adjustments.		

The CMS-contracted auditor will perform audit work on the following areas of FISCAM as part of the CFO Act audits:

Control Activity	Detailed Testing	
Access Controls		
AC-2 Maintain a current list of authorized users and their access authorized.		
1. Resource owners have	1. Review pertinent written policies and procedures.	
identified authorized users and	2. For a selection of users (both application user and	
their access authorized.	<i>IS</i> personnel) review access authorization	
	documentation.	
	3. Interview owners and review supporting	
	documentation. Determine whether inappropriate	
	access is removed in a timely manner.	
	4. For a selection of users with dial-up access, review	
	authorization and justification.	
	5. Interview security managers and review	
	documentation provided to them.	
	6. Review a selection of recent profile changes and	
	activity logs.	
	7. Obtain a list of recently terminated employees from	
	Personnel and, for a selection, determine whether	
	system access was promptly terminated.	
2. Emergency and temporary	1. Review pertinent policies and procedures.	
access authorization is	2. Compare a selection of both expired and active	
controlled.	temporary and emergency authorizations (obtained	
	from the authorizing parties) with a system-	
	generated list of authorized users.	

Control Activity	Detailed Testing
	3. Determine the appropriateness of access
	documentation and approvals and the timeliness of
	terminating access authorization when no longer
	needed.
3. Owners determine disposition	1. Examine standard approval forms.
and sharing of data.	2. Interview data owners.
	3. Examine documents authorizing file sharing and file
	sharing agreements.
AC-3 Establish physical and logi	cal controls to prevent or detect unauthorized access.
	have been implemented. (see also EVA)
A. Passwords, tokens, or other	1. Review pertinent policies and procedures.
devices are used to identify	2. Interview users.
and authenticate users.	3. Review security software password parameters.
	4. Observe users keying in passwords.
	5. Attempt to log on without a valid password; make
	repeated attempts to guess passwords.
	6. Assess procedures for generating and
	communicating passwords to users.
	7. Review a system-generated list of current
	passwords.
	8. Search password file using audit software.
	9. Attempt to log on using common vendor supplied
	passwords.
	10. Interview users and security managers.
	11. Review a list of IDs and passwords.
	12. Repeatedly attempt to log on using invalid
	passwords.
	13. Review security logs.
	14. Review pertinent policies and procedures.
	15. Review documentation of such comparisons.
	16. Interview security managers.
	17. Make comparison using audit software.
	18. View dump of password files (e.g., hexadecimal
	printout).
	19. Interview users.
	20. To evaluate biometrics or other technically
	sophisticated authentication techniques, the auditor
	should obtain the assistance of a specialist.
B. Identification of access paths.	1. Review access path diagram.
C. Logical controls over data	1. Interview security administrators and system users.
files and software	 Review security administration and system about Review security software parameters.
programs.	3. Observe terminals in use.
1 0	5. Cosor ve terminurs in use.

Control Activity	Detailed Testing
	4. Review a system-generated list of inactive logon
	IDs, and determine why access for these users has
	not been terminated.
	5. Determine library names for sensitive or critical
	files and libraries and obtain security reports of
	related access rules. Using these reports, determine
	who has access to critical files and libraries and
	whether the access matches the level and type of
	access authorized.
	6. Perform penetration testing by attempting to access
	and browse computer resources including critical
	data files, production load libraries, batch
	operational procedures (e.g., JCL libraries), source
	code libraries, security software, and the operating
	system. These tests should be performed as (1) an
	"outsider" with no information about the entity's
	computer systems; and (2) an "outsider" with prior
	knowledge about the systemse.g., an ex-insider,
	and (3) an "insider" with and without specific
	information about the entity's computer systems,
	and with access to the entity's facilities.
	7. When performing outsider tests, test the controls
	over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and
	the Internet.
	8. When performing insider tests, use an ID with no
	special privileges to attempt to gain access to
	computer resources beyond those available to the
	account. Also, try to access the entity's computer
	resources using default/generic IDs with easily
	guessed passwords.
	9. Determine whether naming conventions are used.
D. Logical controls over a	1. Review pertinent policies and procedures.
database.	2. Interview database administrator.
	3. Review DBMS and DD security parameters.
	4. Test controls by attempting access to restricted files.
	5. Review security system parameters.
E. Logical controls over	1. Review pertinent policies and procedures.
telecommunications access.	2. Review parameters set by communications software
	or teleprocessing monitors.
	3. Test telecommunications controls by attempting to
	access various files through communications
	networks.

Control Activity	Detailed Testing
	4. Identify all dial-up lines through automatic dialer
	software routines and compare with known dial-up
	access. Discuss discrepancies with management.
	5. Interview telecommunications management staff
	and users.
	6. Review pertinent policies and procedures.
	7. View the opening screen seen by
	telecommunication system users.
	8. Review the documentation showing changes to dial-
	in numbers.
	9. Review entity's telephone directory to verify that the numbers are not listed.
2. Cryptographic tools. (see also	1 To evaluate cryptographic tools, the auditor should
EVA)	obtain the assistance of a specialist.
/	apparent security violations, and take appropriate
remedial action.	apparent security from tons, and take appropriate
1. Audit trails are maintained.	1. Review security software settings to identify types
	of activity logged.
2. Actual or attempted	1. Review pertinent policies and procedures.
unauthorized, unusual, or	2. Review security violation reports.
sensitive access is monitored.	3. Examine documentation showing reviews of
	questionable activities.
3. Suspicious access activity is	1. Test a selection of security violations to verify that
investigated and appropriate	follow-up investigations were performed and to
action is taken.	determine what action were taken against the
	perpetrator.
	2. Interview senior management and personnel
	responsible for summarizing violations.
	3. Review any supporting documentation.
	4. Review policies and procedures and interview
	appropriate personnel.
	5. Review any supporting documentation.
Application Software Developmen	
1. A SDLC has been	ogram modifications are properly authorized.
implemented.	1. Review SDLC methodology.
implementeu.	2. Review system documentation to verify that SDLC methodology was followed.
	3. Interview staff.
	 A. Review training records.
2. Authorizations for software	 Review training records. Identify recent software modifications and
2. Authorizations for software modifications are documented	determine whether change request forms were used.
and maintained.	 Examine a selection of software change request
una muntamoa.	forms for approvals.
	3. Interview software development staff.
	5. Interview software development start.

Co	ontrol Activity	De	tailed Testing
	Use of public domain and	1.	Review pertinent policies and procedures.
	person software is restricted.	2.	Interview users and data processing staff.
C	C-2 Test and approve all new a		
	Changes are controlled as	1.	Review test plan standards.
	programs progress through	2.	For the software change requests selected for
	testing to final approval.		control activity CC-1.2: (1) review specifications;
	0 11		(2) trace changes from code to design
			specifications; (3) review test plans; (4) compare
			test documentation with related test plans; (5)
			analyze test failures to determine if they indicate
			ineffective software testing; (6) review test
			transactions and data; (7) review test results; (8)
			review documentation of management or security
			administrator reviews; (9) verify user acceptance;
			and (10) review updated documentation.
		3.	Determine whether operational systems experience
			a high number of abends and, if so, whether they
			indicate inadequate testing prior to implementation.
2.	Emergency changes are		Review procedures.
	promptly tested and approved.	2.	For a selection of emergency changes recorded in
			the emergency change log, review related
2		1	documentation and approval.
3.	Distribution and		Examine procedures for distributing new software.
	implementation of new or revised software is controlled.	2.	Examine implementation orders for a sample of
			changes.
1.	C-3 Control software libraries. Programs are labeled and	1.	Review pertinent policies and procedures.
1.	inventoried.	1. 2.	
	inventoried.	2. 3.	Interview personnel responsible for library control.
		5.	Examine a selection of programs maintained in the library and assess compliance with prescribed
			procedures.
		4	Determine how many prior versions of software
		1.	modules are maintained.
2.	Access to program libraries is	1.	Examine libraries in use.
	restricted.		Interview library control personnel.
			Examine libraries in use.
			Verify that source code exists for a selection of
			production load modules by (1) comparing compile
			dates, (2) recompiling the source modules, and (3)
			comparing the resulting module size to production
			load modules size.
		5.	For critical software production programs,
			determine whether access control software rules are
			clearly defined.

C	ontrol Activity	De	tailed Testing
		6.	Test access to program libraries by examining
		0.	security system parameters.
		7	Select some program tapes from the log and verify
		/.	the existence of the tapes either in the library or
			with the individual responsible for withdrawing the
			tapes.
3	Movement of programs and	1	Review pertinent policies and procedures.
5.	data among libraries is		
	controlled.	Ζ.	For a selection of program changes, examine related documentation to verify that: (1) procedures for
	controlled.		authorizing movement among libraries were
			followed, and (2) before and after images were
			compared.
Sv	stems Software		compared.
•		two	20
	-1 Limit access to systems soft Access authorizations are		
1.			Review pertinent policies and procedures.
	appropriately limited.	2.	Interview management and systems personnel
		2	regarding access restrictions.
		3.	Observe personnel accessing systems software, such as sensitive utilities, and note the controls
			,
		4	encountered to gain access.
		4.	Attempt to access the operating system and other
		5.	systems software.
		5.	Select some systems programmers and determine whether management-approved documentation
			supports their access to systems software.
		6	Select some application programmers and
		0.	determine whether they are not authorized access.
		7	Determine the last time the access capabilities of
		/.	system programmers were reviewed.
2	All access paths have been	1	Test the operating system parameters to verify that
2.	identified and controls	1.	it is configured to maintain the integrity of the
	implemented to prevent or		security software and application controls.
	detect access for all paths.	2.	Obtain a list of vendor-supplied software and
	detect decess for an paulo.	2.	determine if any of these products have known
			deficiencies that adversely impact the operating
			system integrity controls.
		3.	Judgmentally review the installation of systems
			software components and determine whether they
			were appropriately installed to preclude adversely
			impacting operating system integrity controls.
		4.	Perform an operating system penetration analysis to
			determine if users can inappropriately utilize
			computer resources through direct or covert
			methods including:

Control Activity	Detailed Testing
	(1) Determine whether the operating system's
	subsystems have been appropriately
	implemented to ensure that they support
	integrity controls.
	(2) Determine whether applications interfaces have
	been implemented to support operating system
	integrity controls, including on-line transaction
	monitors; database software; on-line editors; on-
	line direct-access storage devices, on-line
	operating system datasets; exits related to the
	operating system, security, and program
	products; and controls over batch processing, to
	include security controls, scheduler controls,
	and access authorities.
	(3) Evaluate the controls over external access to
	computer resources including networks, dial-up,
	LAN, WAN, RJE, and the Internet.
	(4) Identify potential opportunities to adversely
	impact the operating system and its products
	through trojan horses, viruses, and other
	malicious actions.
	5. Obtain a list of all systems software on test and
	production libraries used by the entity.
	6. Verify that access control software restricts access
	to systems software.
	7. Using security software reports, determine who has
	access to systems software files, security software,
	and logging files. Preferably, reports should be
	generated by the auditor, but at a minimum, they
	shall be generated <i>in</i> the presence of the auditor.
	8. Verify that system programmer's access to production data and programs is only allowed under
	controlled updates and during emergencies when
	established procedures are followed.
	 9. Inquire as to whether disabling has occurred.
	10. Test for default presence using vendor standard IDs
	and passwords.
	11. Determine what terminals are set up as master
	consoles and what controls exist over them.
	12. Test to determine if the master console can be
	accessed or if other terminals can be used to mimic
	the master console and take control of the system.
SS-2 Monitor access to and use	
1. Policies and techniques have	1. Review pertinent policies and procedures.

Control Activity	Detailed Testing
been implemented for using	2. Interview management and systems personnel
and monitoring use of system	regarding their responsibilities.
utilities.	3. Determine whether logging occurs and what
	information is logged.
	4. Review logs.
	5. Using security software reports, determine who can
	access the logging files.
2. Inappropriate or unusual	1. Interview technical management regarding their
activity is investigated and	reviews of privileged systems software and utilities
appropriate actions taken.	usage.
	2. Review documentation supporting their reviews.
	3. Interview management and systems personnel
	regarding these investigations.
	4. Review documentation supporting these
	investigations.
	5. Interview systems programmer supervisors to
	determine their activities related to supervising and
	monitoring their staff.
	6. Review documentation supporting their supervising
	and monitoring of systems programmers' activities.
	7. Interview management and analyze their reviews concerning the use of systems software.
	8. Determine what management reviews have been
	conducted, and their currency, over this area.
SS-3 Control systems software c	
1. Systems software changes are	1. Review pertinent policies and procedures.
authorized, tested, and	2. Interview management and systems personnel.
approved before	3. Review procedures for identifying and documenting
implementation.	systems software problems.
	4. Interview management and systems programmers.
	5. Review the causes and frequency of any recurring
	systems software problems, as recorded in the
	problem log, and ascertain if the change control
	process should have prevented these problems.
	6. Determine what authorizations and documentation
	are required prior to initiating systems software
	changes.
	7. Select recent systems software changes and
	determine whether the authorization was obtained
	and the change is supported by a change request
	document.
	8. Determine the procedures used to test and approve
	systems software prior to its implementation.

Control Activity	Detailed Testing
	 9. Select recent systems software changes and test whether the indicated procedures were in fact used. 10. Review procedures used to control and approve
	emergency changes. 11. Select some emergency changes to systems software and test whether the indicated procedures were in fact used.
2. Installation of systems software is documented and reviewed.	1. Interview management and systems programmers about scheduling and giving advance notices when systems software is installed.
	 Review recent installations and determine whether scheduling and advance notification did occur. Determine whether better scheduling and notification of installations appears warranted to
	 reduce impact on data processing operations. 4. Interview management, systems programmers, and library control personnel, and determine who migrates approved systems software to production libraries and whether outdated versions are removed from production libraries.
	 5. Review supporting documentation for some systems software migrations and the removal of outdated versions from production libraries.
	 Interview data center management about their role in reviewing systems software installations.
	 7. Review some recent systems software installations and determine whether documentation shows that logging and management review occurred.
	 Interview systems software personnel concerning a selection of systems software and determine the extent to which the operating version of the systems software is currently supported by the vendor.
	9. Interview management and systems programmers about the currency of systems software and the currency and completeness of software documentation.
	10. Review documentation and test whether recent changes are incorporated.

Co	ontrol Activity	_	tailed Testing		
Se	ction I: Risk Assessment Review	W			
A.	Determine if the current	1.	Review the most recent system configuration		
	system configuration is	2.	Review the system configuration and/or related		
	documented, including links to		documentation indicating it has been reviewed and		
	other systems.		kept current		
В.	Determine if <i>RA</i> s are	1.	Review the <i>RA</i> policies		
	performed and documented on	2.	Review the most recent <i>RA</i>		
	an annual basis or whenever	3.	Review the <i>RA</i> and/or related documentation		
	the system, facilities, or other		indicating it has been reviewed and conducted		
	conditions change.		annually		
C.	Determine if data sensitivity	1.	Review data classification policies and procedures		
	and integrity of the data have	2.	Review evidence based on policies and procedures		
	been documented and if data		that data has been classified		
	has been classified				
D.	Determine if threat sources,	1.	Review <i>RA</i> to ensure that threat sources, both		
	both natural and manmade,		natural and man-made, have been identified and		
_	have been formally identified		documented.		
E.	Determine if a list of known	1.	Review the <i>RA</i> to ensure that a list of known system		
	system vulnerabilities, system		vulnerabilities, system flaws, or weaknesses that		
	flaws, or weaknesses that could		could be exploited by threat sources has been		
	be exploited by threat sources	2	developed.		
	has been developed and	2.	Review the <i>RA</i> and/or related documentation		
Б	maintained current. Determine if an analysis has	1	indicating it has been reviewed and kept current.		
г.	been conducted that determines	1.	Review the <i>RA</i> to ensure that mitigating controls are documented.		
	whether the security	2	Review the <i>RA</i> to ensure that mitigating controls		
	requirements in place	۷.	have been assessed and documented to determine if		
	adequately mitigate		they adequately mitigate vulnerabilities.		
	vulnerabilities.		they adequately initigate varietabilities.		
G.	Determine if final risk	1.	Review the <i>RA</i> to ensure that final risk		
	determinations and related		determinations are documented.		
	management approvals have	2.	Review <i>RA</i> and/or related documentation indicating		
	been documented and		it has been approved (currently).		
	maintained on file.				
H.	Determine if a	1.	Review documented critical business processes.		
	mission/business impact	2.	Review mission/business impact analysis to ensure		
	analysis have been conducted		that it has been documented for the critical business		
	and documented.		processes		
I.	Obtain management's list of	1.	Review any additional documented lists of controls		
	additional controls that have		identified to mitigate identified risks.		
	been identified to mitigate				
G	identified risks.				
Se	Section II: Policies and Procedures to Reduce Risk				

Table D-3. Detailed MMA 912 Testing Procedures

Control A	Activity	De	tailed Testing	
	the policies and		Review the most current <i>RA</i> .	
	dures for IT security to		Review IT Security policies and procedures to	
-	nine if there is a		ensure that they reduce the risk outlined in the <i>RA</i> .	
docum	nent that outlines	3.	Ensure that IT Security policies and procedures are	
reduci	ng the risk exposures		current.	
	fied in Roman numeral I			
above				
B. Detern	mine if management	1.	Review the most current <i>SDLC</i> .	
activit	ies include security	2.	Review additional information (i.e., <i>SSP</i>) which	
contro	ols in the costs of		outline security controls included in the cost of	
develo	pping new systems as		developing new systems	
part of	f their SDLC. Determine	3.	Review software change control policies and	
if proc	cedures for software		procedures to ensure that changes are being	
chang	es include steps to		controlled effectively.	
contro	ol the changes.		-	
C. Deterr	mine if management has	1.	Perform inquiries of appropriate personnel	
perfor	med accreditations and		regarding major systems maintained at the site.	
certifi	cations of major systems	2.	Review documentation indicating accreditations	
	ordance with FISMA		and certifications were performed for the noted	
	es, including security		systems.	
	ols testing and	3.	Ensure that accreditations and certifications are in	
	nentation.		compliance with FISMA policies .	
	nine the number of	1.	Perform inquiries of appropriate personnel	
•	ns for which security		regarding systems for which controls have been	
	ols have been tested and		tested.	
	ated. Determine if the	2.	Review evidence (i.e., internal/external audits)	
-	n/network boundaries		indicating system controls have been tested and	
	been subjected to periodic		evaluated for the identified systems.	
review	vs/audits.	3.	Review evidence (i.e., internal/external penetration	
			tests, etc) indicating system/network boundaries	
			have been subjected to periodic reviews/audits.	
		4.	Ensure that all reviews have been performed within	
	1 1 0	4	the scope of the review.	
	the results of		Review the most recent CMS CSR.	
	gement's compliance	2.	GAPs in compliance as documented in the CMS	
	list with the CMS CSR to		CSR.	
detern	determine gaps in compliance.	3.	Review management's response to the CSR to	
			ensure that proper controls are in place/are in the	
		1	process of being in place.	
	mine if security policies	1.	Review platform security configuration policies and	
-	ocedures include	~	procedures.	
	ols to address platform	2.	Review patch management policies and procedures.	
	ty configurations, and			
	management.	• .		
Section III: Review of System Security Plans				

Co	ntrol Activity	De	tailed Testing
	Determine if a security plan is		Review most current <u>SSP</u> .
	documented and approved.	2.	Review documentation indicating the <i>SSP</i> was approved by appropriate individuals.
В.	Determine if the plan is kept current.		Review previous and current <i>SSP</i> to ensure that updates have been made as necessary. Review the date of the most current <i>SSP</i> to ensure
		2.	that it is in the scope of the review.
C.	Determine if a security management structure has been established.	1.	Review the security management's organizational chart.
D.	Determine if <i>IS</i> responsibilities are clearly assigned.		Review the security management's organization chart. Review the security management's formal job
			descriptions.
E.	Determine if owners and users	1.	Review security training schedules.
	are aware of security policies.	2.	Review security training materials.
		3.	For a selection of owners and users ensure that they
-		4	have attended the required trainings.
F.	Determine if security policies		Review the most current <i>SDLC</i> .
	and procedures are included in the policies and procedures for control of the life cycle of	2.	Review additional <i>SDLC</i> policies and procedures to ensure that security polices and procedures have been incorporated.
	systems, including accreditations and		Perform inquiries of appropriate personnel regarding major systems maintained at the site
	certifications.	4.	Review documentation indicating accreditations and certifications were performed for the noted systems.
G.	Determine if hiring, transfer, termination and performance	1.	Review hiring policies and procedure to ensure that they address security.
	policies address security.	2.	Review transfer policies and procedures to ensure that they address security.
		3.	Review termination policies and procedures to ensure that they address security.
		4.	Review performance policies and procedures (i.e., R <i>OB</i> and Performance Evaluations) to ensure they address security.
H.	Determine if employee background checks are	1.	Review policies and procedures for performing background checks.
	performed.	2.	Select a sample of employees and ensure that background investigations have been completed.
I.	Determine if security employees have adequate	1.	Identify all employees responsible for administering security.

Co	ntrol Activity	De	tailed Testing
	security training and expertise.	2.	Review training records and certifications for all security employees to ensure that adequate training has been received.
J.	Determine if management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of security policies and procedures.	1.	Review policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures. Review documentation indicating management has periodically reviewed, updated, and approved security policies and procedures.
K.	Determine if management ensures that corrective actions are effectively implemented.		Review policies and procedures for ensuring that corrective actions are effectively implemented. Review evidence that management ensures that corrective actions are effectively implemented.
Se	ction IV: Review of Security Av	ware	eness Training
	Determine if employees have received a copy of the <i>ROB</i> .	1.	Inquire of the appropriate personnel regarding the maintenance and distribution of the <i>ROB</i> for all types of employees.
			Review the most current version of the <i>ROB</i> . Select a sample of employees and ensure that they have received a copy of the most current version of the <i>ROB</i> .
	Determine if employee training and professional development has been documented and formally monitored.	3.	Inquire of the appropriate personnel regarding the documentation and formal monitoring of employee training and professional development. Review policies and procedures regarding the documentation and formal monitoring of employee training and professional development. For a selected sample of employees, review evidence that training and professional development is documented and formally monitored.
C.	Determine if there is mandatory annual refresher training for security.	2.	Review policies and procedures regarding mandatory annual refresher security training. Review the most recent security awareness training curriculum. For a selected sample of employees, review evidence that all attended the mandatory annual refresher security training.
D.	Determine if systemic methods are employed to make employees aware of security, i.e., posters, booklets, etc.		Review policies and procedures regarding methods to make employees aware of security. Conduct a walk through of the site to ensure that posters/flyers are in fact hanging in visible areas. Inspect evidence that methods to make employees aware of security are implemented.

Control Activity	Detailed Testing
E. Determine if employees have received a copy of or have easy access to agency security procedures and policies.	 Inquire of appropriate personnel regarding employee access to agency security procedures and policies. Inspect evidence that employees have received a copy or have easy access to the agency security procedures and policies. Review policies and procedures in which employees have easy access to ensure that they are the most current.
F. Determine if security professionals have received specific training for their job responsibilities and the type and frequency of application- specific training provided to employees and contractor personnel is documented and tracked.	 Identify all employees responsible for administering security. Review training records and certifications for all security employees to ensure that adequate training has been received. Inquire of appropriate personnel regarding the documentation and tracking of application specific training for employees. Review the most recent application specific training curriculum. Inspect evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked.
Section V: Review of periodic test policies	ting and evaluation of the effectiveness of IT security
A. Determine if management reports for the review and testing of IT security policies and procedures, including network <i>RA</i> , accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	1. Inspect evidence that periodic testing of IT security policies and procedures (including network <i>RAs</i> , accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted.
B. Determine if annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	 Inspect evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.
C. Determine if remedial action is being taken for issues noted on	1. Review policies and procedures for taking remedial action for issues noted on audits.

Co	ontrol Activity	De	tailed Testing
Se	audits.	2.	Inspect evidence that Corrective Action Plans including remedial actions being taken for the issues noted on audits is being documented and monitored. vities, processes, and reporting for deficiencies
	Determine if weaknesses are clearly tracked in a formal database or other manner and that action is planned to address all IT security weaknesses.	1. 2.	Review policies and procedures regarding the tracking of identified weaknesses, including actions for addressing the IT security weakness. Inspect evidence that weaknesses are tracked in a formal database (or other manner). Inspect evidence that planned actions to address all IT security weaknesses is being tracked.
B.	Read the CAP to determine corrective actions have been taken by management to address IT security weaknesses.		Review policies and procedures for preparing the CAP. Review all quarterly CAPs that were performed during the scope of the review to ensure that corrective actions have been taken to address IT security weaknesses.
C.	Determine the number and nature of security IT weaknesses for which corrective action has been delayed and determine if management have provided explanations as to why.		Review policies and procedures for preparing CAPs. Review all quarterly CAPs that were performed during the scope of the review to determine the number of corrective actions that have been delayed. Inspect evidence that management has provided an explanation as to why the corrective action has been delayed for all noted in the CAP.
Se	ction VII: Review of Incident D	etec	
	Determine that management has processes to monitor systems and the network for unusual activity, and/or intrusion attempts.	1.	Review policies and procedures for monitoring systems and networks for unusual activity, and or intrusion attempts. Inspect evidence that management is monitoring systems and networks for unusual activity and/or intrusion attempts based on the policies and procedures.
B.	Determine if management has procedures to take and has taken action in response to unusual activity, intrusion attempts and actual intrusions.		Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur. Inspect evidence that management has taken action in response to unusual activity, intrusion attempts, and/or actual intrusions if any have occurred within the scope of the review.
C.	Determine that management processes and procedures include reporting of intrusion	1.	Review polices and procedures to be followed in the event unusual activity, intrusion attempts, and actual intrusions occur.

Co	ntrol Activity	De	tailed Testing
	attempts and intrusions in		Ensure that that policies and procedures are in
	accordance with FISMA		accordance with FISMA standards.
	guidance.		
See	ction VIII: Policies and procedu	ures	for continuity of operations and related physical
	curity safeguards for IT systems		
A.	Determine if critical data and	1.	Review the Business Contingency Plan to ensure
	operations are formally		that critical data and operations are formally
	identified and prioritized.		identified and prioritized.
В.	Determine if resources	1.	Review the Business Contingency Plan to ensure
	supporting critical operations		that resources supporting critical operations are
	are identified in contingency		identified.
	plans.		
C.	Determine if emergency	1.	Review emergency processing priorities to ensure
	processing priorities are		that they are formally documented.
	established.		
D.	Determine if data and program	1.	Review data and program backup policies and
	backup procedures have been	-	procedures.
	implemented.	2.	Inspect evidence (i.e., backup logs) that data and
			program backup procedures have been
Б	Datamaina if a da quata	1	implemented.
E.	Determine if adequate environmental controls have	1.	Inquire of data center manager concerning the environmental controls implemented in the data
	been implemented.		center.
		2	Perform Walkthrough of data center to ensure that
		2.	adequate environmental controls have been
			implemented.
F.	Determine if staff have been	1.	Review emergency response policies and
	trained to respond to		procedures.
	emergencies.	2.	Review emergency response training curriculum.
	6	-	Inspect evidence that emergency response training
			has been provided for applicable staff.
G.	Determine that hardware	1.	Ensure that hardware maintenance procedures exist
	maintenance, problem		to help prevent unexpected interruptions.
	management, and change	2.	Ensure that problem management procedures exist
	management procedures exist		to help prevent unexpected interruptions.
	to help prevent unexpected	3.	Ensure that change management procedures exist to
	interruptions.		help prevent unexpected interruptions.
H.	Determine if policies and	1.	Review policies and procedures regarding the
	procedures for disposal of data		disposal of data and equipment to ensure that
	and equipment exist and		applicable Federal security and privacy
	include applicable Federal		requirements are included.
	security and privacy		
	requirements.		

Control Activity	Detailed Testing
I. Determine if an up-to-date contingency plan is documented.	1. Inspect evidence that the contingency plan was approved within the scope of the review.
J. Determine if arrangements have been made for alternate data processing and telecommunications facilities.	 Review the contingency plan to ensure that arrangements have been made for alternate data processing and telecommunications facilities. Review the contract with the organization that will provide alternate data processing and telecommunications operations if necessary.
K. Determine if the plan is periodically tested.	 Review policies and procedures regarding periodically testing the contingency plan. Inspect evidence that the contingency plan has been periodically tested.
L. Determine if the results are analyzed and contingency plans adjusted accordingly.	1. Inspect evidence that the contingency plan is adjusted accordingly after the tests are performed and analyzed.
M. Determine if physical security controls exist to protect IT resources.	1. Inquire of data center manager concerning the physical security controls implemented in the data center.
	2. Perform Walkthrough of data center to ensure that adequate physical security controls exist.

	Table D-4. Detailed SAS 70 Testing Procedures		
Co	ntrol Activity	Detailed Testing	
A. 1	A.1 An entity-wide security program has been documented, approved and monitored by management in accordance with the CMS Business Partners Systems Security Manual (BPSSM) and includes requirements to assess security risks periodically, establish a security management structure and clearly assign security responsibilities, implement effective security-related personnel policies, monitor the security program's effectiveness and ensure security officer training and employee security awareness.		
1.	A security plan is documented and approved.	 Reviewed the security plan. Determined whether the plan covers the topics prescribed by OMB Circular A-130. 	
2.	The security plan is kept current.	 Reviewed the security plan and any related documentation indicating that it has been reviewed, updated and is current. 	
3.	A security management structure has been established.	 Reviewed the security plan and the entity's organization chart. Interviewed security management staff. Reviewed pertinent organization charts and job descriptions. 	
4.	LS responsibilities are clearly assigned.	 Reviewed the security plan. Reviewed the security management's organization chart. Reviewed the security management's formal job descriptions. 	
5.	Owners and users are aware of security policies.	 Reviewed documentation supporting or evaluating the awareness program. Observed a security briefing. Interviewed data owners and system users. Determined what training they have received and if they are aware of their security-related responsibilities. Reviewed memos, electronic mail files, or other policy distribution mechanisms. Reviewed personnel files to test whether security awareness statements are current. Called selected users, identified yourself as security or network staff, and attempted to talk them into revealing their password. Reviewed security training schedules. Reviewed security training materials. For a selection of owners and users ensured that they have attended the required trainings. 	
6.	Management periodically assesses the appropriateness of	 Reviewed the reports resulting from recent assessments, including the most recent FMFIA 	

Control Activity	Detailed Testing
security policies and	report.
compliance with them.	2. Determined when last independent review or audit
	occurred and reviewed results.
	3. Reviewed written authorizations or accreditation
	statements.
	4. Reviewed documentation related to corrective
	actions.
	5. Reviewed policies and procedures regarding the
	periodic assessment of the appropriateness of
	security policies and procedures.
	6. Reviewed documentation indicating management
	has periodically reviewed, updated, and approved
	security policies and procedures.
7. Employees have adequate	1. Reviewed job descriptions for security management
training and expertise.	personnel, and for a selection of other personnel.
	2. For a selection of employees, compared personnel
	records on education and experience with job
	descriptions.
	3. Reviewed training program documentation.
	4. Reviewed training records and related
	documentation showing whether such records are monitored and whether employees are receiving the
	appropriate training.
8. Employee training and	1. Inquired of the appropriate personnel regarding the
professional development has	documentation and formal monitoring of employee
been documented and formally	training and professional development.
monitored.	2. Reviewed policies and procedures regarding the
	documentation and formal monitoring of employee
	training and professional development.
	3. For a selected sample of employees, reviewed
	evidence that training and professional development
	is documented and formally monitored.
9. There is mandatory annual	1. Reviewed policies and procedures regarding
refresher training for security.	mandatory annual refresher security training
	2. Reviewed the most recent security awareness
	training curriculum.
	3. For a selected sample of employees, reviewed
	evidence that all attended the mandatory annual
10. Sustania matheda an	refresher security training.
10. Systemic methods are	1. Reviewed policies and procedures regarding
employed to make employees	methods to make employees aware of security.
aware of security, i.e., posters, booklets, etc.	2. Conducted a walk through of the site to ensure that posters/flyers are in fact hanging in visible areas.
	3. Inspected evidence that methods to make employees
	aware of security are implemented.

Control Activity	Detailed Testing
11. Employees have received a copy of or have easy access to agency security procedures and policies.	 Inquired of appropriate personnel regarding employee access to agency security procedures and policies. Inspected evidence that employees have received a copy or have easy access to the agency security procedures and policies. Reviewed policies and procedures in which employees have easy access to ensure that they are
background investigations an agreements with employees (1	 the most current. Identified all employees responsible for administering security. Reviewed training records and certifications for all security employees to ensure that adequate training has been received. Inquired of appropriate personnel regarding the documentation and tracking of application specific training for employees. Reviewed the most recent application specific training curriculum. Inspected evidence that employees requiring application specific training are receiving it, as well as it being documented and tracked. dicies are implemented that include performance of d contacting references, include confidentiality regular, contractual and temporary) and include cedures that require exit interviews, return of
	O cards, notification to security management of ess to systems and escorting of terminated employees
 Hiring, transfer, termination, and performance policies address security. 	 Reviewed hiring policies and procedure to ensure that they address security. Reviewed transfer policies and procedures to ensure that they address security. Reviewed termination policies and procedures to ensure that they address security. Ensured that performance policies and procedures (i.e., <i>ROB</i> and Performance Evaluations) address security. Reviewed reinvestigation policies. Reviewed policies and procedures for performing background checks. For a selection of sensitive positions, inspected personnel records and determined whether background reinvestigations have been performed. Reviewed policies on confidentiality or security

Control Activity	Detailed Testing
Control Activity	agreements.
	9. For a selection of such users, determined whether
	confidentiality or security agreements are on file.
	10.Reviewed vacation policies.
	11.Inspected personnel records to identify individuals who have not taken vacation or sick leave in the
	past year.
	12.Determined who performed vacationing employee's work during vacation.
	13.Reviewed job rotation policies.
	14. Reviewed staff assignment records and determined
	whether job and shift rotations occur. 15.Reviewed pertinent policies and procedures.
	16. For a selection of terminated or transferred
	employees, examined documentation showing compliance with policies.
	17.Compared a system-generated list of users to a list
	of active employees obtained from personnel to
	determine if IDs and passwords for terminated
	employees exist.
2. Management has documented	1. Reviewed policies and procedures regarding the
that they periodically assess the	periodic assessment of the appropriateness of
appropriateness of security	security policies and procedures.
policies and compliance with	2. Reviewed documentation indicating management
them, including testing of	has periodically reviewed, updated, and approved
security policies and	security policies and procedures.
procedures.	
3. Employees have received a	1. Inquired of the appropriate personnel regarding the
copy of the <i>ROB</i> .	maintenance and distribution of the <i>ROB</i> for all
	types of employees.
	2. Reviewed the most current version of the <i>ROB</i> .
	3. Selected a sample of employees and ensured that
	they have received a copy of the most current
	version of the <i>ROB</i> .
	assified (risk-ranked) according to their
· · · · ·	periodically formally reviewed.
1. Resource classifications and	1. Reviewed data classification policies and
related criteria have been established.	procedures.
	2. Interviewed resource owners.
2. Owners have classified	1. Reviewed resource classification documentation
resources.	and compared to <i>RA</i> s. Discussed any discrepancies with appropriate officials
2 Data appointivity and into arity	with appropriate officials.
3. Data sensitivity and integrity	1. Reviewed evidence based on policies and
have been documented and data	procedures that data has been classified.

Control Activity	Detailed Testing
has been classified.	
appropriately author resource owners, pro	ed applications, systems software, and Medicare data is ized, documented, and monitored, and includes approval by cedures to control emergency and temporary access, and and properly dispose of data.
1. Resource owners have	1. Reviewed pertinent written policies and procedures.
identified authorized use their access authorized.	
	 documentation. Determined whether inappropriate access is removed in a timely manner. 4. For a selection of users with dial-up access,
	 5. Interviewed security managers and reviewed
	documentation provided to them.6. Reviewed a selection of recent profile changes and
	 activity logs. 7. Obtained a list of recently terminated employees from Personnel and, for a selection, determined whether system access was promptly terminated.
2. Emergency and tempora access authorization is controlled.	 Reviewed pertinent policies and procedures. Compared a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users. Determined the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer
3. Owners determine dispo	needed.
and sharing of data.	 Examined standard approval forms. Interviewed data owners. Examined documents authorizing file sharing and file sharing agreements.
4. Sanitation of equipment media prior to disposal or reuse.	and 1. Reviewed written procedures.
5 Access outhorizations	 4. For selected items still in the entity's possession, tested that they have been appropriately sanitized. 1. Deviation and procedures recording the
5. Access authorizations an appropriately limited.	re 1. Reviewed policies and procedures regarding the disposal of data and equipment to ensure that

Control Activity	Detailed Testing
	applicable Federal security and privacy
	requirements are included.
	2. Interviewed management and systems personnel
	regarding access restrictions.
	3. Observed personnel accessing systems software,
	such as sensitive utilities, and noted the controls
	encountered to gain access.
	4. Attempted to access the operating system and other
	systems software.
	5. Selected some systems programmers and
	determined whether management-approved
	documentation supports their access to systems
	software.
	6. Selected some application programmers and
	determined whether they are not authorized access.
	7. Determined the last time the access capabilities of
	system programmers were reviewed.
6. Passwords, tokens, or other	1. Reviewed pertinent policies and procedures.
devices are used to identify and	2. Reviewed security software password parameters.
authenticate users.	3. Observed users keying in passwords.
	4. Attempted to log on without a valid password; make
	repeated attempts to guess passwords.
	5. Assessed procedures for generating and
	communicating passwords to users.
	6. Reviewed a system-generated list of current
	passwords.7. Searched password file using audit software.
	 Searched password me using audit software. 8. Attempted to log on using common vendor supplied
	passwords.
	9. Interviewed users and security managers.
	10.Reviewed a list of IDs and passwords.
	11.Repeatedly attempted to log on using invalid
	passwords.
	12.Reviewed security logs.
	13.Reviewed pertinent policies and procedures.
	14.Reviewed documentation of such comparisons.
	15.Interviewed security managers.
	16.Made comparison using audit software.
	17. Viewed dump of password files (e.g., hexadecimal
	printout).
	18.To evaluate biometrics or other technically
	sophisticated authentication techniques, the auditor
	obtained the assistance of a specialist.
7. Identification of access paths.	1. Reviewed access path diagram.
	1. 1. 1. in the decess putil diagram.

Control Activity	Detailed Testing
8. Logical controls over data files	1. Interviewed security administrators and system
and software programs.	users.
	2. Reviewed security software parameters.
	3. Observed terminals in use.
	4. Reviewed a system-generated list of inactive logon
	IDs, and determined why access for these users has
	not been terminated.
	5. Determined library names for sensitive or critical
	files and libraries and obtained security reports of
	related access rules. Using these reports, determined
	who has access to critical files and libraries and
	whether the access matches the level and type of
	access authorized.
	6. Performed penetration testing by attempting to access and browse computer resources including
	critical data files, production load libraries, batch
	operational procedures (e.g., JCL libraries), source
	code libraries, security software, and the operating
	system.
	7. When performing outsider tests, tested the controls
	over external access to computer resources,
	including networks, dial-up, LAN, WAN, RJE, and
	the Internet.
	8. When performing insider tests, used an ID with no
	special privileges to attempt to gain access to
	computer resources beyond those available to the
	account. Also, tried to access the entity's computer
	resources using default/generic IDs with easily
	guessed passwords.
0 Logical controls over a	 9. Determined whether naming conventions are used. 1. Reviewed pertinent policies and procedures.
9. Logical controls over a database.	 Reviewed pertinent poncies and procedures. Interviewed database administrator.
database.	3. Reviewed DBMS and DD security parameters.
	 Reviewed DBWS and DD security parameters. Tested controls by attempting to access restricted
	files.
	5. Reviewed security system parameters.
10. Logical controls over	1. Reviewed security system parameters.
telecommunications access.	 Reviewed permitter ponetes and procedures. Reviewed parameters set by communications
	software or teleprocessing monitors.
	3. Tested telecommunications controls by attempting
	to access various files through communications
	networks.
	4. Identified all dial-up lines through automatic dialer
	software routines and compared with known dial-up

Control Activity	Detailed Testing
	access. Discussed discrepancies with management.
	5. Interviewed telecommunications management staff
	and users.
	6. Reviewed pertinent policies and procedures.
	7. Viewed the opening screen seen by
	telecommunication system users.
	8. Reviewed the documentation showing changes to
	dial-in numbers.
	9. Reviewed entity's telephone directory to verify that
	the numbers are not listed.
11. Cryptographic tools.	1. To evaluate cryptographic tools, the auditor
	obtained the assistance of a specialist.
A.5 Security policies and proced	ures include controls to ensure the security of
platform configurations and	to ensure proper patch management of operating
systems.	
1. All access paths have been	1. Tested the operating system parameters to verify
identified and controls	that it is configured to maintain the integrity of the
implemented to prevent or	security software and application controls.
detect access for all paths.	2. Obtained a list of vendor-supplied software and
	determined if any of these products have known
	deficiencies that adversely impact the operating
	system integrity controls.
	3. Judgmentally reviewed the installation of systems
	software components and determined whether they
	were appropriately installed to preclude adversely
	impacting operating system integrity controls.
	4. Performed an operating system penetration analysis
	to determine if users can inappropriately utilize computer resources through direct or covert
	methods.
	5. Obtained a list of all systems software on test and
	production libraries used by the entity.
	6. Verified that access control software restricts access
	to systems software.
	7. Using security software reports, determined who
	has access to systems software files, security
	software, and logging files. Preferably, reports
	should be generated by the auditor, but at a
	minimum, they <i>shall</i> be generated In the presence
	of the auditor.
	8. Verified that system programmer's access to
	production data and programs is only allowed under
	controlled updates and during emergencies when
	established procedures are followed.
	9. Inquired whether disabling has occurred.

Co	ontrol Activity	Detailed Testing
	v	10. Tested for default presence using vendor standard
		IDs and passwords.
		11.Determined what terminals are set up as master
		consoles and what controls exist over them.
		12. Tested to determine if the master console can be
		accessed or if other terminals can be used to mimic
		the master console and take control of the system.
2.	Security policies and	1. Reviewed platform security configuration policies
	procedures include controls to	and procedures.
	address platform security	2. Reviewed patch management policies and
	configurations, and patch	procedures.
	management.	1
3.	Annual reviews and audits are	1. Inspected evidence that annual reviews and audits
	conducted to ensure	of IT security controls (including logical and
	compliance with FISMA	physical security controls, platform configuration
	guidance from OMB for	standards, and patch management controls) are
	reviews of IT security controls,	conducted to ensure compliance with FISMA.
	including logical and physical	
	security controls, platform	
	configuration standards and	
	patch management controls.	
A.		ees, including visitors, to Medicare facilities, data
		priately authorized, documented, and access
1	violations are monitored and	
1.	Physical safeguards have been established that are	1. Reviewed a diagram of the physical layout of the
	commensurate with the risks of	computer, telecommunications, and cooling system facilities.
	physical damage or access.	2. Performed a walkthrough of data center to ensure
	physical damage of access.	that adequate physical security controls exist.
		3. Reviewed lists of individuals authorized access to
		sensitive areas and determined the appropriateness
		for access.
		4. Before becoming recognized as the auditor,
		attempted to access sensitive areas without escort or
		identification badges.
		5. Observed entries to and exits from facilities during
		and after normal business hours.
1		6. Observed utilities access paths.
		7. Inquired of data center manager concerning the
		physical security controls implemented in the data
		center.
		8. Observed entries to and exits from sensitive areas
		8. Observed entries to and exits from sensitive areas

Co	ontrol Activity	Detailed Testing
	e e	10.Selected from the log some returns and
		withdrawals, verified the physical existence of the
		tape or other media, and determined whether proper
		authorization was obtained for the movement.
		11.Observed practices for safeguarding keys and other
		devices.
		12.Reviewed written emergency procedures.
		13.Examined documentation supporting prior fire
		drills.
		14.Observed a fire drill.
2.	Visitors are controlled.	1. Reviewed visitor entry logs.
		2. Observed entries to and exits from sensitive areas
		during and after normal business hours.
		3. Interviewed guards at facility entry.
		4. Reviewed documentation on and logs of entry code
		changes.
		5. Observed appointment and verification procedures
		for visitors.
3.	Actual or attempted	1. Reviewed pertinent policies and procedures.
	unauthorized, unusual, or	2. Reviewed security violation reports.
	sensitive access is monitored.	3. Examined documentation showing reviews of
		questionable activities.
4.	Suspicious access activity is	1. Tested a selection of security violations to verify
	investigated and appropriate	that follow-up investigations were performed and to
	action is taken.	determine what actions were taken against the
		perpetrator.
		2. Interviewed senior management and personnel
		responsible for summarizing violations.
		3. Reviewed any supporting documentation.
5.	Physical security controls exist	1. Inquired of data center manager concerning the
	to protect IT resources.	physical security controls implemented in the data
		center.
		2. Performed walkthrough of data center to ensure that
<u> </u>		adequate physical security controls exist.
6.	Physical and logical access	1. Interviewed management and subordinate
	controls have been established.	personnel.
A.		ated systems software development and maintenance
1		umented, tested, and approved.
1.	Authorizations for software	1. Identified recent software modifications and
	modifications are documented	determined whether change request forms were
	and maintained,	used.
		2. Examined a selection of software change request
		forms for approvals.
		3. Interviewed software development staff.

Control Activity	Detailed Testing
2. Emergency changes are	1. Reviewed procedures.
promptly tested and approved.	2. For a selection of emergency changes recorded in
	the emergency change log, reviewed related
	documentation and approval.
3. Systems software changes are	1. Reviewed pertinent policies and procedures.
authorized, tested, and	2. Interviewed management and systems personnel.
approved before	3. Reviewed procedures for identifying and
implementation.	documenting systems software problems.
-	4. Interviewed management and systems
	programmers.
	5. Reviewed the causes and frequency of any recurring
	systems software problems, as recorded in the
	problem log, and ascertain if the change control
	process should have prevented these problems.
	6. Determined what authorizations and documentation
	are required prior to initiating systems software
	changes.
	7. Selected recent systems software changes and
	determined whether the authorization was obtained
	and the change is supported by a change request
	document.
	8. Determined the procedures used to test and approve
	systems software prior to its implementation.
	9. Selected recent systems software changes were
	tested to verify indicated procedures were in fact
	used.
	10. Reviewed procedures used to control and approve
	emergency changes.
	11.Selected some emergency changes to systems
	software and tested whether the indicated
	procedures were in fact used.
4. Installation of systems software	1. Interviewed management and systems programmers
is documented and reviewed.	about scheduling and giving advance notices when
	systems software is installed.
	2. Reviewed recent installations and determine
	whether scheduling and advance notification did
	occur.
	3. Determined whether better scheduling and
	notification of installations appears warranted to
	reduce impact on data processing operations.
	4. Interviewed management, systems programmers,
	and library control personnel, and determined who migrates approved systems software to production
	libraries and whether outdated versions are removed
	from production libraries.

Control Activity	Detailed Testing
Control Activity	 Detailed Testing 5. Reviewed supporting documentation for some systems software migrations and the removal of outdated versions from production libraries. 6. Interviewed data center management about their role in reviewing systems software installations. 7. Reviewed some recent systems software installations and determined whether documentation shows that logging and management review occurred. 8. Interviewed systems software personnel concerning
	 a selection of systems software and determined the extent to which the operating version of the systems software is currently supported by the vendor. 9. Interviewed management and systems programmers about the currency of systems software and the currency and completeness of software documentation. 10.Reviewed documentation and tested whether recent
 5. Management activities include security controls in the costs of double include activities are part 	changes are incorporated.1. Reviewed the most current System Development Life Cycle.
developing new systems as part of their SDLC. Determine if procedures for software changes include steps to control the changes.	 Reviewed additional information (i.e., <i>SSP</i>) which outline security controls included in the cost of developing new systems. Reviewed software change control policies and procedures to ensure that changes are being controlled effectively.
6. Management has performed accreditations and certifications of major systems in accordance with FISMA policies, including security controls testing and documentation.	 Performed inquiries of appropriate personnel regarding major systems maintained at the site. Reviewed documentation indicating accreditations and certifications were performed for the noted systems. Ensured that accreditations and certifications are in compliance with FISMA policies .
v i	Cycle methodology is documented and in use and
	ts for security requirements in systems.
1. A SDLC has been implemented.	 Reviewed SDLC methodology. Reviewed system documentation to verify that SDLC methodology was followed. Interviewed staff. Reviewed training records.
2. Management activities include security controls in the costs of developing new systems as part	 Reviewed additional information (i.e., <i>SSP</i>) which outline security controls included in the cost of developing new systems.

Co	ntrol Activity	Detailed Testing
	of their SDLC. Determine if procedures for software changes include steps to control the changes.	2. Reviewed software change control policies and procedures to ensure that changes are being controlled effectively.
3.	Security policies and procedures are included in the policies and procedures for control of the life cycle of systems, including accreditations and certifications.	 Reviewed additional System Development Life Cycle policies and procedures to ensure that security polices and procedures have been incorporated. Performed inquiries of appropriate personnel regarding major systems maintained at the site. Reviewed documentation indicating accreditations and certifications were performed for the noted systems
A.9 Change management policies and procedures exist that include documented		
testing and approval of changes for regular and emergency changes and		
1		ic domain and personal software.
1.	Authorizations for software modifications are documented and maintained.	 Identified recent software modifications and determined whether change request forms were used.
		 Examined a selection of software change request forms for approvals. Interviewed software development staff.
2.	Use of public domain and	1. Reviewed pertinent policies and procedures.
	personal software is restricted.	2. Interviewed users and data processing staff.
3.	e	1. Reviewed test plan standards.
	programs progress through testing to final approval.	 For the selected software change requests (1) reviewed specifications; (2) traced changes from code to design specifications; (3) reviewed test plans; (4) compared test documentation with related test plans; (5) analyzed test failures to determine if they indicate ineffective software testing; (6) reviewed test transactions and data; (7) reviewed test results; (8) reviewed documentation of management or security administrator reviews; (9) verified user acceptance; and (10) reviewed updated documentation. Determined whether operational systems experienced a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
4.	Emergency processing	1. Reviewed emergency processing priorities to ensure
5.	priorities are established. Data and program backup procedures have been	 that they are formally documented. Reviewed data and program backup policies and procedures.
	implemented.	2. Inspected evidence (i.e., backup logs) that data and

Control Activity	Detailed Testing
	program backup procedures have been
	implemented.
6. Hardware maintenance,	1. Reviewed hardware maintenance procedures that
problem management, ar	id exist to help prevent unexpected interruptions.
change management	2. Reviewed problem management procedures that
procedures exist to help	prevent exist to help prevent unexpected interruptions.
unexpected interruptions	. 3. Reviewed change management procedures that exist
	to help prevent unexpected interruptions.
A.10 Access to program lib among libraries is cor	raries is properly restricted and movement of programs itrolled.
1. Programs are labeled and	
inventoried.	2. Interviewed personnel responsible for library
	control.
	3. Examined a selection of programs maintained in the
	library and assessed compliance with prescribed
	procedures.
	4. Determined how many prior versions of software
	modules are maintained.
2. Access to program librar	
restricted.	2. Interviewed library control personnel.
	3. Verified that source code exists for a selection of
	production load modules.
	4. For critical software production programs,
	determined whether access control software rules
	are clearly defined.
	5. Tested access to program libraries by examining
	security system parameters.
	6. Selected some program tapes from the log and
	verified the existence of the tapes either in the
	library or with the individual responsible for withdrawing the topos
3. Movement of programs a	withdrawing the tapes.und1. Reviewed pertinent policies and procedures.
data among libraries is	2. For a selection of program changes, examined
controlled.	related documentation to verify that: (1) procedures
controned.	for authorizing movement among libraries were
	followed, and (2) before and after images were
	compared.
A.11 Adequate segregation	of duties exists between various functions within Medicare
	ported by appropriately authorized and documented policies.
1. Incompatible duties have	
identified and policies	2. Interviewed selected management and <i>IS</i> personnel
implemented to segregate	
1 1	
duties.	3. Reviewed an agency organization chart showing <i>IS</i>

Control Activity	Detailed Testing
	4. Interviewed selected personnel and determined
	-
	whether functions are appropriately segregated.
	5. Determined whether the chart is current and each
	function is staffed by different individuals.
	6. Reviewed relevant alternate or backup assignments
	and determined whether the proper segregation of
	duties is maintained.
	7. Observed activities of personnel to determine the
	nature and extent of the compliance with the
	intended segregation of duties.
	8. Reviewed the organizational chart and interviewed
	personnel to determine that assignments do not
	result in a single person being responsible for the
	indicated combination of functions.
	9. Determined through interview and observation
	whether data processing personnel and security
	managers are prohibited from these activities.
	10.Reviewed the adequacy of documented operating
	procedures for the data center.
2. Job descriptions have been	1. Reviewed job descriptions for several positions in
documented.	organizational units and for user security
	administrators.
	2. Determined whether duties are clearly described
	and prohibited activities are addressed.
	3. Reviewed the effective dates of the position
	descriptions and determined whether they are
	current.
	4. Compared these descriptions with the current
	responsibilities and duties of the incumbents in
	these positions to determine the accuracy of these
	statements.
	5. Reviewed job descriptions and interviewed
	management personnel.
3. Employees understand their	1. Interviewed personnel filling positions for the
	selected job descriptions (see above). Determined if
duties and responsibilities.	5 1 7
	the descriptions match their understanding of their duties and responsibilities and whether additional
	duties and responsibilities and whether additional duties are undertaken that are not listed in their job
	duties are undertaken that are not listed in their job
	descriptions.
	2. Determined from interviewed personnel whether
	senior management has provided adequate
	resources and training to establish, enforce, and
	institutionalize the principles of segregation of
	duties.
	3. Interviewed management personnel in these

Control Activity Detailed Testing		Detailed Testing
		activities.
4.	Management reviews	1. Interviewed management and subordinate
	effectiveness of control	personnel.
	techniques.	2. Selected documents or actions that require
		supervisory review and approval for evidence of
		such performance (e.g., approval of input of
		transactions, software changes).
		3. Determined which reviews are conducted to assess
		the adequacy of duty segregation. Obtained and
		reviewed results of such reviews.
5.	Formal procedures guide	1. Reviewed manuals.
	personnel in performing their	2. Interviewed supervisors and personnel.
	duties.	3. Observed processing activities.
6.	Active supervision and review	1. Interviewed supervisors and personnel.
	are provided for all personnel.	2. Observed processing activities.
		3. Reviewed history log reports for signatures
		indicating supervisory review.
		4. Determined who is authorized to perform the <i>IPL</i>
		for the system, what steps are followed, and what
		controls are in place to monitor console activity
		during the process. Determined whether operators
		override the IPL parameters.
A.		d be controlled via formal operating procedures that
		vee activities by management with documentation
		ce of management's monitoring and review process.
1.	Audit trails are maintained.	1. Reviewed security software settings to identify
		types of activity logged.
2.	Actual or attempted	1. Reviewed pertinent policies and procedures.
	unauthorized, unusual, or	2. Reviewed security violation reports.
	sensitive access is monitored.	3. Examined documentation showing reviews of
		questionable activities.
3.	Policies and techniques have	1. Reviewed pertinent policies and procedures.
	been implemented for using	2. Interviewed management and systems personnel
	and monitoring use of system	regarding their responsibilities.
	utilities.	3. Determined whether logging occurs and what
		information is logged.
		4. Reviewed logs.
		5. Using security software reports, determined who
		can access the logging files.
4.	Inappropriate or unusual	1. Interviewed technical management regarding their
	activity is investigated and	reviews of privileged systems software and utilities
	appropriate actions taken.	usage.
		2. Reviewed documentation supporting their reviews.
1		3. Interviewed management and systems personnel

Co	ontrol Activity	Detailed Testing
	v	regarding these investigations.
		4. Reviewed documentation supporting these
		investigations.
		5. Interviewed systems programmer supervisors to
		determine their activities related to supervising and
		monitoring their staff.
		6. Reviewed documentation supporting their
		supervising and monitoring of systems
		programmers' activities.
		7. Interviewed management and analyzed their
		reviews concerning the use of systems software.
		8. Determined what management reviews have been
		conducted, and their currency, over this area.
5.	Formal procedures guide	1. Reviewed manuals.
	personnel in performing their	2. Interviewed supervisors and personnel.
	duties.	3. Observed processing activities.
6.	Active supervision and review	1. Interviewed supervisors and personnel.
	are provided for all personnel.	2. Observed processing activities.
		3. Reviewed history log reports for signatures
		indicating supervisory review.
	system vulnerabilities, system threat sources.	ssessment includes identification of threats, known n flaws, or weaknesses that could be exploited by
1.	Risks are periodically assessed.	1. Reviewed <i>RA</i> policies.
		2. Reviewed the most recent high-level <i>RA</i> .
		3. Reviewed the objectivity of personnel who
		performed and reviewed the assessment.
2.	The current system	1. Reviewed the most recent system configuration.
	configuration is documented,	2. Reviewed the system configuration and/or related
	including links to other	documentation indicating it has been reviewed and
	systems.	kept current.
3.	Data sensitivity and integrity of	1. Reviewed data classification policies and
		1 1
	the data have been documented	procedures
	the data have been documented and if data have been classified.	2. Reviewed evidence based on policies and
1	and if data have been classified.	 Reviewed evidence based on policies and procedures that data have been classified
4.	and if data have been classified. Threat sources, both natural	 Reviewed evidence based on policies and procedures that data have been classified Reviewed <i>RA</i> to ensure that threat sources, both
4.	and if data have been classified. Threat sources, both natural and manmade, have been	 Reviewed evidence based on policies and procedures that data have been classified Reviewed <i>RA</i> to ensure that threat sources, both natural and man-made, have been identified and
	and if data have been classified. Threat sources, both natural and manmade, have been formally identified.	 Reviewed evidence based on policies and procedures that data have been classified Reviewed <i>RA</i> to ensure that threat sources, both natural and man-made, have been identified and documented.
	and if data have been classified. Threat sources, both natural and manmade, have been formally identified. A list of known system	 Reviewed evidence based on policies and procedures that data have been classified Reviewed <i>RA</i> to ensure that threat sources, both natural and man-made, have been identified and documented. Reviewed the <i>RA</i> to ensure that a list of known
	and if data have been classified. Threat sources, both natural and manmade, have been formally identified. A list of known system vulnerabilities, system flaws, or	 Reviewed evidence based on policies and procedures that data have been classified Reviewed <i>RA</i> to ensure that threat sources, both natural and man-made, have been identified and documented. Reviewed the <i>RA</i> to ensure that a list of known system vulnerabilities, system flaws, or weaknesses
	and if data have been classified. Threat sources, both natural and manmade, have been formally identified. A list of known system	 Reviewed evidence based on policies and procedures that data have been classified Reviewed <i>RA</i> to ensure that threat sources, both natural and man-made, have been identified and documented. Reviewed the <i>RA</i> to ensure that a list of known

Control Activity	Detailed Testing
been developed and maintained	2. Reviewed the <i>RA</i> and/or related documentation
current.	indicating it has been reviewed and kept current.
6. An analysis has been conducted	1. Reviewed the <i>RA</i> to ensure that mitigating controls
that determines whether the	are documented.
security requirements in place	2. Reviewed the <i>RA</i> to ensure that mitigating controls
adequately mitigate	have been assessed and documented to determine if
vulnerabilities.	they adequately mitigate vulnerabilities.
7. Final risk determinations and	1. Reviewed the <i>RA</i> to ensure that final risk
related management approvals	determinations are documented.
have been documented and	2. Reviewed <i>RA</i> and/or related documentation
maintained on file.	indicating it has been approved (currently).
8. A mission/business impact	1. Reviewed documented critical business processes.
analysis have been conducted	2. Reviewed mission/business impact analysis to
and documented.	ensure that it has been documented for the critical
	business processes.
9. Obtain management's list of	1. Reviewed any additional documented lists of
additional controls that have	controls identified to mitigate identified risks.
been identified to mitigate	
identified risks.	
10. Determine the number of	1. Performed inquiries of appropriate personnel
systems for which security	regarding systems for which controls have been
controls have been tested and	tested.
evaluated. Determine if the	2. Reviewed evidence (i.e., internal/external audits)
system/network boundaries	indicating system controls have been tested and
have been subjected to periodic	evaluated for the identified systems.
reviews/audits.	3. Reviewed evidence (i.e., internal/external
	penetration tests, etc) indicating system/network
	boundaries have been subjected to periodic
	reviews/audits.
	4. Ensured that all reviews have been performed
	within the scope of the review.
e	nt focal point for IT RA has been established that
-	s programs, processes and procedures to mitigate
	ses to assess the effectiveness of risk mitigation
programs.	1. Deviand the approximation and distribution
1. A security management	1. Reviewed the security plan and the entity's
structure has been established.	organization chart.
	2. Interviewed security management staff.
	3. Reviewed pertinent organization charts and job
	descriptions.
2 IS reapongibiliting and algority	4. Interviewed the security manager.
2. <i>IS</i> responsibilities are clearly	1. Reviewed the security plan.
assigned. 3. Final risk determinations and	1. Reviewed the <i>RA</i> to ensure that final risk
related management approvals	determinations are documented.
related management approvais	עלולווווומווטווא מול עטלעווולווולע.

Control Activity		Detailed Testing		
	have been documented and	2. Reviewed <i>RA</i> and/or related documentation		
	maintained on file.	indicating it has been approved (currently).		
4.	Obtain management's list of additional controls that have been identified to mitigate identified risks.	 Reviewed any additional documented lists of controls identified to mitigate identified risks. 		
5.	Read the policies and	1. Reviewed the most current <i>RA</i> .		
5.	procedures for IT security to determine if there is a document that outlines reducing the risk exposures identified in Roman numeral I above.	 Reviewed IT Security policies and procedures to ensure that they reduce the risk outlined in the <i>RA</i>. Ensured that IT Security policies and procedures are current. 		
6.	Management has documented that they periodically assess the appropriateness of security policies and compliance with them, including testing of	 Reviewed policies and procedures regarding the periodic assessment of the appropriateness of security policies and procedures. Reviewed documentation indicating management has periodically reviewed, updated, and approved 		
	security policies and procedures.	security policies and procedures.		
7.	Management reports for the review and testing of IT security policies and procedures, including network <i>RA</i> , accreditations and certifications, internal and external audits and security reviews and penetration and vulnerability assessments exist.	1. Inspected evidence that periodic testing of IT security policies and procedures (including network <i>RA</i> s, accreditations and certifications, internal and external audits, security reviews, and penetration and vulnerability assessments) have been conducted.		
8.	Annual reviews and audits are conducted to ensure compliance with FISMA guidance from OMB for reviews of IT security controls, including logical and physical security controls, platform configuration standards and patch management controls.	1. Inspected evidence that annual reviews and audits of IT security controls (including logical and physical security controls, platform configuration standards, and patch management controls) are conducted to ensure compliance with FISMA.		
Α.		mented, approved, and monitored by management in		
		Risk Assessment and System Security Plan		
1	Procedures.	1 Deviewed DA policies		
1.	Risks are periodically assessed.	1. Reviewed <i>RA</i> policies.		
		2. Reviewed the most recent high-level <i>RA</i> .		
		3. Reviewed the objectivity of personnel who performed and reviewed the assessment.		

Co	ntrol Activity	Detailed Testing
	A security plan is documented	1. Reviewed the security plan.
	and approved.	2. Determined whether the plan covers the topics
	11	prescribed by OMB Circular A-130.
3.	The plan is kept current.	1. Reviewed the security plan and any related
		documentation indicating that it has been reviewed
		and updated and is current.
A.1	6 Regularly scheduled processe	s required to support the Medicare contractor's
		, facilities or equipment) are performed.
1.	Data and program backup	1. Reviewed written policies and procedures for
	procedures have been	backing up files.
	implemented.	2. Compared inventory records with the files
	-	maintained off-site and determined the age of these
		files.
		3. For a selection of critical files, located and
		examined the backup files. Verified that backup
		files can be used to recreate current reports.
		4. Determined whether backup files are created and
		rotated off-site as prescribed and are sent before
		prior versions are returned.
		5. Located and examined documentation.
		6. Examined the backup storage site.
2.	Adequate environmental	1. Examined the entity's facilities
	controls have been	2. Interviewed site managers.
	implemented.	3. Observed that operations staff are aware of the
		locations of fire alarms, fire extinguishers, regular
		and auxiliary electrical power switches, water shut-
		off valves, breathing apparatus, and other devices
		that they may be expected to use in an emergency.
		4. Observed the operation, location, maintenance and
		access to the air cooling system.
		5. Observed whether water can enter through the
		computer room ceiling or pipes are running through
		the facility and that there are water detectors on the \tilde{x}
		floor.
		6. Determined whether the activation of heat and
2	0.001	smoke detectors will notify the fire department.
	Staff have been trained to	1. Interviewed data center staff.
	respond to emergencies.	2. Reviewed training records.
		3. Reviewed training course documentation.
		4. Reviewed emergency response procedures.
		5. Reviewed test policies.
		6. Reviewed test documentation.
		7. Interviewed data center staff.
4.	Effective hardware	1. Reviewed hardware maintenance procedures.

Co	ntrol Activity	De	etailed Testing
	maintenance, problem		Reviewed problem management procedures.
	management, and change		Reviewed change management procedures.
	management procedures exist.		
A. 1		ent	process is in place that includes planning,
			Illy documenting remedial action addressing
			uudits and reviews of IT systems, components and
	operations.	•	
1.	Management ensures that	1.	Reviewed the status of prior-year audit
	corrective actions are		recommendations and determined if implemented
	effectively implemented.		corrective actions have been tested.
	• •	2.	Reviewed recent FMFIA reports.
			Reviewed policies and procedures for ensuring that
			corrective actions are effectively implemented.
		4.	Reviewed evidence that management ensures that
			corrective actions are effectively implemented.
2.	Read the results of	1.	Reviewed the most recent CMS CSR.
	management's compliance	2.	Noted GAPs in compliance as documented in the
	checklist with the CMS CSR to		CMS CSR.
	determine gaps in compliance.	3.	Reviewed management's response to the CSR to
			ensure that proper controls are in place/are in the
			process of being in place.
3.	Weaknesses are clearly tracked	1.	Reviewed policies and procedures regarding the
	in a formal database or other		tracking of identified weaknesses, including actions
	manner and that action is		for addressing the IT security weakness.
	planned to address all IT	2.	Inspected evidence that weaknesses are tracked in a
	security weaknesses.		formal database (or other manner).
		3.	Inspected evidence that planned actions to address
			all IT security weaknesses are being tracked.
4.	Read the CAP to determine	1.	Reviewed policies and procedures for preparing
	corrective actions have been		CAPs.
	taken by management to	2.	Reviewed all quarterly CAPs that were performed
	address IT security weaknesses.		during the scope of the review to ensure that
			corrective actions have been taken to address IT
			security weaknesses.
5.	The number and nature of	1.	Reviewed policies and procedures for preparing
	security IT weaknesses for		CAPs.
	which corrective action has	2.	Reviewed all quarterly CAPs that were performed
	been delayed and determine if		during the scope of the review to determine the
	management have provided		number of corrective actions that have been
	explanations as to why.		delayed.
		3.	Inspected evidence that management has provided
			an explanation as to why the corrective action has
			been delayed for all noted in the CAP.
6.	Remedial action is being taken	1.	Reviewed policies and procedures for taking
	for issues noted on audits.		remedial action for issues noted on audits.

Control Activity	Detailed Testing
	2. Inspected evidence that Corrective Action Plans
	including remedial actions being taken for the
	issues noted on audits is being documented and
	monitored.
A 18 Management has processes to	monitor systems and the network for unusual
activity and/or intrusion atter	•
1. An incident response capability	1. Interview security manager, response team
has been implemented.	members, and system users.
has been implemented.	 Review documentation supporting incident handling
	activities.
	3. Determine qualifications of response team
	members.
2. Audit trails are maintained.	1. Review security software settings to identify types
2. Fladit fulls are maintained.	of activity logged.
A.19 Management procedures are	in place to ensure proper action in response to
	tempts, and actual intrusions.
1. Suspicious access activity is	1. Reviewed polices and procedures to be followed in
investigated and appropriate	the event unusual activity, intrusion attempts, and
action is taken.	actual intrusions occur.
	2. Tested a selection of security violations to verify
	that follow-up investigations were performed, and
	to determine what actions were taken against the
	perpetrator.
	3. Interviewed senior management and personnel
	responsible for summarizing violations.
	4. Reviewed any supporting documentation.
	5. Reviewed policies and procedures and interviewed
	appropriate personnel.
	6. Reviewed any supporting documentation.
2. Inappropriate or unusual	1. Interviewed technical management regarding their
activity is investigated and	reviews of privileged systems software and utilities
appropriate actions taken.	usage.
	2. Reviewed documentation supporting their reviews.
	3. Interviewed management and systems personnel
	regarding these investigations.
	4. Reviewed documentation supporting these
	investigations.
	5. Interviewed systems programmer supervisors to
	determine their activities related to supervising and
	monitoring their staff.
	6. Reviewed documentation supporting their
	supervising and monitoring of systems
	programmers' activities.
	7. Interviewed management and analyzed their

Control Activity	Detailed Testing	
	reviews concerning the use of systems software.	
	8. Determined what management reviews have been	
conducted, and their currency, over this area.		
A.20 Management processes and procedures include reporting of intrusions attempts		
and intrusions in accordance with the Federal Information Security Management		
Act (FISMA)		
1. Management processes and	1. Reviewed polices and procedures to be followed in	
procedures include reporting of	the event unusual activity, intrusion attempts, and	
intrusion attempts and	actual intrusions occur.	
intrusions in accordance with	2. Ensured that policies and procedures are in	
FISMA guidance.	accordance with FISMA standards.	

Appendix E: CMS Guidelines

1 Introductory Comments to CMS Guidelines on Information Technology Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

1.1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

This document provides introductory comments for a series of guidelines issued by the Centers for Medicare and Medicaid Services (CMS) to assist with the proper understanding and implementation of key security controls around CMS' data and information systems environment. The guidelines issued consist of the following:

- 1) Logical access controls and segregation of duties
- 2) Development and implementation of an entity-wide security plan
- 3) Application programmers' access to application data and source code and application programmer segregation of duties
- 4) Change management procedures and requirements for maintaining change management documentation
- 5) Testing process for the SANS Top 20 Internet Security Vulnerabilities
- 6) Implementation of security configuration templates

The intended audience of these guidelines, however, extends beyond CMS management and staff to include all CMS business partners.

Today's highly technology-dependent organization, while benefiting from the increased capabilities offered by continued improvements in Information Technology (IT), is also faced with the challenge of maintaining sufficient controls around the increased complexities of new developments in IT. The primary objectives of these controls are to maintain confidentiality, integrity, and availability around information critical to the organization's mission.

The six (δ) guidelines mentioned above will provide CMS management and business partners with the information required to ensure that key *Federal* government recommended controls pertaining to each of the six topics are fully incorporated into CMS' current controls management environment.

1.2 Compliance Criteria

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The IT *controls* discussed in the guidelines are part of the foundation of operating in a secure environment promoting effective controls around data confidentiality, integrity, and availability. The importance of these controls is evidenced by the direct inclusion or indirect references to these controls in numerous *Federal* government Acts, standards, and guidelines, including, but not limited to, the following:

- Chief Financial Officers (CFO) Act of 1990
- Federal Financial Management Improvement Act (FFMIA) of 1996
- Federal Manager's Financial Integrity Act of 1982
- Federal Information Security Management Act (FISMA) of 2002
- Various *Office of Management and Budget* (OMB) circulars including OMB A-127 (Financial Management Systems) and OMB A-130 (Security of Federal Automated Information Resources)
- Various *National Institute of Standards and Technology* (NIST) Special Publications (*SP*) in the 800-series reports, and
- *General Accounting Office* (GAO)/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM)

The guidelines focus on the identification and description of controls pertaining to each of the six (6) control areas as recommended by FISCAM and FISMA (and other *Federal* government or industry standards, as required). Listed below is a brief discussion of the compliance framework for FISCAM and FISMA:

- A key goal of the *CFO* Act of 1990 was the development of a consistent approach to financial statement audits of *Federal* government agencies. *The* GAO Financial Audit Manual (FAM) provides detailed guidance on the performance of financial statement audits. In January of 1999, GAO issued the FISCAM as a companion to FAM. FISCAM provides the methodology for IT controls review within the framework of a financial statement audit of *Federal* government agencies.
- In February 2005, NIST published SP 800-53 and in December 2007, NIST SP 800-53 Revision 2to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002. According to the OMB memorandum titled "Memorandum for Heads of Executive Departments and Agencies", dated June 13, 2005, the guidelines documented in NIST SP 800-53 (as amended) are to be used by agencies for selecting security controls for information systems supporting the executive agencies of the Federal government.

The six (6) control areas discussed in the guidelines have manifested themselves within the management practices of CMS through the inclusion of a number of controls related to these areas in CMS' Business Partners Systems Security Manual (BPSSM). CMS has used OMB circulars, NIST Special Publication 800-series reports, and other *Federal* and industry guidelines to compile the IT management practices documented in BPSSM. Included in these practices are specific measures for the implementation of *Core Security R*equirements (*CSR*). All controls listed in the BPSSM are mandatory for all *CMS* business partners. As such, the content of the BPSSM *shall* not be viewed as "guidance'. They are, rather, "requirements" for all CMS business partners.

1.3.1 Year-round Cyclical Approach

(*Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08*)

Controls which are enforced through a periodic assessment against a static controls checklist will inevitably fail. Both the operations environment and the IT environment which supports it are fluid as are the security controls required to ensure data confidentiality, integrity, and availability. As such, the implementation of any control at CMS can only be effective if it is an integral part of the management process. This means incorporation of security controls in the year-round enterprise-wide management lifecycle of the organization.

FISCAM and NIST *SP* 800-53 (*as amended*) have each defined specific roles and responsibilities and an approach to planning and management of effective IT systems security. Within sections 2 and 3 of the BPSSM, CMS has also documented detailed descriptions of system security roles and responsibilities, and an approach to managing IT systems security.

CMS management is committed to ensuring that:

- Sections 2 and 3 of the BPSSM are continually evaluated against the IT security management approach and roles and responsibilities listed in FISCAM and NIST SP 800-53 to facilitate full compliance with these standards; and
- The BPSSM is continually evaluated for compliance with guidance in FISCAM and NIST SP 800-53 regarding specific systems to be covered by the security management program.

Table E-1 maps the key components of the IT security management approach recommended by FISCAM to those recommended by NIST *SP* 800-53 (*as amended*) and those required by BPSSM.

1.3.2 Management Involvement

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

As mentioned in the prior section, effective implementation of IT security controls can only be achieved if it is incorporated in the year-round enterprise-wide management lifecycle at the highest levels of an organization. This requires direct involvement, not only by the IT management structure (e.g., Chief Technology Officer and Chief Information Security Officer) but also by executives at the enterprise-wide level (e.g., program managers and agency leadership). This requirement is not only reflected in the compliance criteria used for the guidelines (e.g., the reporting requirements for FISMA) but also in other IT-related government publications and standards (e.g., the revised OMB Circular A-123, effective FY 2006).

FISCAM	NIST 800-53	BPSSM (includes Chapter #)
Assess Risks	Periodic risk assessments	3.10 Management Security
& Determine		Resources
Needs		
		3.2 Risk Assessment
Implement	System security plans	3.1 System Security Plan
Policies and		
Controls	Policies and procedures based (on the risk	3.4 IT Systems Contingency
	assessments) and subordinate plans for	Plan
	providing adequate system security	
		3.8 Fraud Control
	Plans and Procedures to Ensure	
	Continuity of Operations for IT Systems	3.9 Patch Management
Promote	Security awareness training	Attachment A Core Set of
Awareness		Security Requirements
Monitor &	Periodic testing and evaluation of the	3.3 Certification
Evaluate	effectiveness of IT security policies and	
Policy and	procedures, including:	3.5.1 Annual Compliance Audit
Control		
Effectiveness	Network assessments	3.5.2 Plan of Action and
	Penetration activities	Milestones
	Change management procedures	
	Other	3.6 Incident Reporting and Response
	Remedial activities, processes and	-
	reporting for deficiencies	3.7 System Security Profile
	Incident detection, reporting, and response	

Table E-1. Mapping of IT Security Program Management Principles

1.3.3 Reporting Requirements

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Given the fact that FISCAM's intended audience is financial statement auditors (i.e., Inspector Generals (IG) and independent auditors), it contains no reporting requirements directed specifically at agency management. FISMA however, contains specific reporting requirements for agency management as well as the IG.

According to the OMB Memorandum for Heads of Executive Departments and Agencies, published on June 13, 2005, regarding FISMA reporting instructions, "all agencies *shall* implement the requirements of FISMA and report annually to the *OMB* and Congress on the effectiveness of their security programs." According to the memorandum, each agency head's annual report *shall* be submitted to the Director of OMB and should comprise:

- A transmittal letter from the agency head, including a discussion of any differences between the findings of the agency *Chief Information Officer* (CIO) and IG
- Results of annual IT security reviews of systems and programs [completed by the CIO]
- Results of the IG's independent evaluation [completed by the IG]
- Status of agency compliance with OMB privacy policies [completed by the senior agency official for privacy]

The memorandum states that, prior to submission of the report, the CIO and IG assessment results need to be reconciled to resolve discrepancies, if any, between the two sections. *A* Plan of Action and Milestones (POA&M) *shall* be developed by each agency to correct weaknesses identified in the above reporting process. Reports documenting FISMA compliance updates *shall* be sent by the agency to OMB on a quarterly basis.

The memorandum emphasizes the fact that FISMA applies to information systems used or operated by an agency or by a contractor of the agency or other organization on behalf of the agency. It also states that agencies *shall* report both at an agency-wide level as well as by individual component. Clearly, the FISMA requirements apply to CMS *b*usiness *p*artners listed in the Introduction

In the CMS control environment, the BPSSM discusses a tool to *assist* CMS business partners conduct systems security *evaluation*. It is known as the *FISMA Evaluation (FE)* which is a module in the CMS Integrated Security Suite (CISS) tool. This module assists business partners to *perform their annual FISMA security control validation*. Upon completion of *the FE*, the business partner is required to submit the database to the CMS Central Office, the Consortium Contractor Management Officer and/or CMS Project Officer (CCMO/PO) [along with other required security documentation which is

described in section 3 of the BPSSM]. For CMS business partners, Joint Signature Memorandum JSM-05352, dated 05-17-05, specifies that POA&M reporting is to be performed on a monthly basis.

It is critical that the security review and reporting cycle prescribed by BPSSM follow a time table that allows for timely input to the FISMA reporting process and deadlines mentioned above.

1.4 Conclusion

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The primary objectives of effective IT controls are to maintain confidentiality, integrity, and availability *for* information critical to the organization's mission. Through the implementation of effective IT *c*ontrols security vulnerabilities can be reduced, security risks can be mitigated, and breaches in security can be identified and corrected in a timely manner. Examples of such security risks include theft and fraud. The implementation of the controls discussed in the six (6) guidelines, however, should be part of an enterprise-wide operational approach rather than a technology-centric approach and should, thus, be incorporated in the highest levels of management planning and enforcement practices within CMS. This, of course, necessitates the direct involvement of management at the highest levels of the organization (not just technology management).

Given the dynamic nature of CMS' operational needs and the technology supporting these needs, the re-assessment, modification, and re-design of CMS' security management and control practices as well as the testing and monitoring of compliance with these practices must be an on-going process to ensure new operational and technology developments and the resulting security vulnerabilities are effectively addressed.

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective IT controls is security and a key foundation of comprehensive security controls is **logical access controls and segregation of duties**. This guideline *shall*:

- Provide a high level understanding of **logical access controls and segregation of duties**,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related to **logical access controls and segregation of duties**, and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

2.2 Introduction to Logical Access Controls and Segregation of Duties

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The BPSSM defines access controls as "the process of granting or denying specific requests to: (i) obtain and use information and related information processing services; and (ii) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances)."

According to FISCAM, key objectives of logical access controls are to ensure that: (1) users have only the access needed to perform their duties, (2) access to very sensitive resources, such as security software programs, is limited to very few individuals, and (3) employees are restricted from performing incompatible functions or functions beyond their responsibility.

FISCAM states that "If these objectives are met, the risk of inappropriate modification or disclosure of data can be reduced without interfering with the practical needs of users. However, establishing the appropriate balance between user needs and security requires a careful analysis of the criticality and sensitivity of information resources available and the tasks performed by users."

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers (IDs), passwords, or other identifiers that are linked to predetermined access privileges. Controls should be designed to restrict legitimate users to the specific systems, programs, and files needed to perform their duties while inhibiting access by others.

FISCAM defines "segregation of duties" as controls that describe how work responsibilities should be segregated so that one person does not have access to or control

over all of the critical stages of an information handling process. For instance; while representatives of the user community may initiate requests for changes to system capabilities, computer programmers should not be allowed to write, test, and approve program changes; and a user who has entered transactions in the system, should not have the capability to also review and approve the processing of all such transactions. Often, proper segregation of duties is achieved by splitting responsibilities between two or more organizational groups to ensure independence and objective checks and balances. Controls can be enforced through automated and/or manual measures.

2.3 Risks of Non-compliance

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Per FISCAM, "inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure and modification of data". Following are examples, extracted from FISCAM, which illustrate the potential consequences of such vulnerabilities.

- By obtaining direct access to **data files**, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could: (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) inadvertently or purposefully change a receivable balance, or (4) obtain confidential information about business transactions or individuals.
- By obtaining access to **application programs** used to process transactions, an individual could make unauthorized changes to these programs or introduce malicious programs, which in turn could be used to access data files, resulting in situations similar to those describe above, or to process unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for himself or herself.
- By obtaining access to **computer facilities and equipment**, an individual could: (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.

FISCAM states that "inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed." FISCAM provides the following examples of potential consequences of inadequate controls around segregation of duties:

• *An* individual who was independently responsible for authorizing processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or

• *A* computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Within appendix C of the BPSSM, CMS outlines a number of specific safeguards against employee fraud. **Segregation of duties** is listed as a key safeguard against employee fraud. For a more detailed look into each of the measures for the prevention and detection of fraudulent activities see appendix C of the BPSSM.

2.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place which satisfy the control objective.**

Table E-3 and Table E-4 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to **logical access controls and segregation of duties**. Refer to Chapter 3 of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-3. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-4.

The FISMA compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare claims processing systems and Medicare data center systems be categorized as "high impact" security systems.

As mentioned above, Table E-4 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to **logical access controls and segregation of duties**. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-4 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-4, the corresponding FISCAM control in Table E-3, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) include the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with **logical access controls and segregation of duties** guidelines.

2.5 Sample Instances of Non-Compliance and Recommended Resolution

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Table E-2 below provides a listing of sample instances of non-compliance with logical access controls and segregation of duties based on prior controls reviews and audits. Specifically, the table lists the findings, issues and recommended course of action for selected cases of non-compliance. The findings and issues in this table are not exhaustive in that they do not list ALL prior instances of non-compliance at all CMS sites. A sample of prior audit findings and issues have been selected instead in order to give the reader a sense of "real world" cases of prior control issues found at various CMS locations while avoiding repetition of similar issues found at different CMS sites. It should also be noted that the recommendation for each issue takes into account the business operations and technology environment of a specific CMS site. Consequently, the recommendation listed in the table for a specific issue may not apply to all sites.

Finding	Issue	Suggested Remediation
Password management controls need to be strengthened	 Some user accounts were not set to force the use of a combination of alphabetical, numeric, and/or special characters. 	Force RACF password configuration settings to include a combination of alphabetical, numeric, and/or special characters (may require an exit).

Table E-2. Sample Findings from Prior CMS Controls Reviews and Audits

Finding	Issue	Suggested Remediation
	2. Management does not have a process for periodically reviewing user ID profiles to ensure that these profiles are not configured with inappropriate settings.	Periodically review user accounts and passwords to ensure that they adhere to BPSSM requirements and applicable FISCAM Controls and Control Techniques, e.g., access settings reflect job responsibilities, use of alpha-numeric passwords, etc. These controls can be enforced through, manual as well as automated, means.
Logical access controls need to be strengthened	1. Revoked RACF user IDs are not being promptly removed from the mainframe system.	Clarify and document the programs, processes, and procedures used to periodically review and remove "revoked" user IDs from the system. Document and maintain justifications for revoked RACF user IDs on the system, as well as, authorizations for the reactivation or deletion of these accounts.
	2. Access to the DB2 system, which contains sensitive Medicare information, is not being restricted to users on a "need to know" basis.	Update the database administration policies and procedures to include comprehensive processes and procedures regarding the maintenance of documented RACF user authorizations to access DB2 data sets containing sensitive Medicare data. Document and maintain authorizations for all RACF user IDs with access to DB2 data sets containing sensitive Medicare data. Develop, document, and implement processes and procedures to monitor user accesses to sensitive Medicare data maintained in DB2 data sets and to take appropriate action when questionable access is detected.
Resource owners have not identified or granted access to authorized users.	 No user access documentation exists for network devices, including the Cisco router and the Cisco PIX firewall. Access to the Cisco routers and the Cisco PIX firewall are not proactively monitored. Logging is disabled on the Cisco PIX firewall. 	Continue efforts in developing a logging and monitoring strategy for Cisco routers and Cisco PIX firewalls. The strategy should be implemented on the Medicare systems and throughout the organization. A policy should also be developed to outline roles and responsibilities in ensuring that the systems are configured correctly and that logs are being generated and reviewed. A formal user access policy should be complied with for granting users access to all network devices including Cisco routers and Cisco PIX firewalls.

Finding	Issue	Suggested Remediation
Oracle database control deficiencies	 A process for establishing the accounts is not defined and documented. 	Develop and document procedures for establishing Oracle accounts.
	2. The defined privileges are not periodically assessed and revalidated.	Develop and document procedures for reviewing Oracle accounts, account privileges, and user roles.
	3. Procedures for assigning user roles have not been documented.	Develop and document procedures for assigning user roles.
	4. Oracle logs are not reviewed and automated tools to assist in log reviews do not exist.	Develop and document procedures for reviewing Oracle logs. Research and implement automated tools to assist in log reviews and monitoring.
	5. The configuration setting to provide log actions performed by privileged accounts was not set.	Configure the Oracle initialization file to generate audit logs of actions performed by privileged users.
Improvements in Password controls over network devices that allow Dial- in access	1. Noted poor password controls for devices that allow access to the network. As a result, passwords could be easily guessed.	Management should establish, implement, and enforce formal policies and procedures for remote access password-use ensuring that "hard-to-guess" passwords are required for authentication of remote users.
Password Parameters did not meet CMS Core Security Requirements	 For the mainframe, the following ACF2 password settings were used: 1. PSWD HISTORY = NO Activates default history of one generation. Old passwords may be used after one generation 2. MIN PSWD LENGTH = 5 - Allowed five characters for a minimum. 	ACF2 policies should be improved to meet the minimum requirements outlined in the CMS Core Security Requirements. Correct and resubmit CMS CAST worksheets to reflect the current environment.

Finding	Issue	Suggested Remediation
Job rotation and vacation policy does not exist	 3. LOGON RETRY COUNT = 3 - Does not deactivate the user ID after three failed passwords, but rather logs the terminal session off. The user can immediately restart the session and conduct additional logon attempts. 4. MAX PSWD ATTEMPTS = 6 - Allows a user ID to have six invalid password attempts during a password change period, at which time the account is locked out. A formal policy mandating periodic job rotations and vacation for personnel does not exist. 	We recommend that management incorporate a formal job rotation and vacation policy so that responsibilities can be re-assigned to different individuals. Should neither of the above two measures exist, we recommend the monitoring of employee activities who are exposed to sensitive data over extended periods in order to reduce potential security risks.

2.6 **Periodic Review and Testing of Controls**

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems, and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time. Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be reassessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is the **development and implementation** of an entity-wide security plan. This guideline *shall*:

- Provide a high level understanding of the **development and implementation of an entity-wide security plan**,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related to the **development and implementation of an entity-wide security plan**, and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

3.2 Introduction to the Development and Implementation of an Entity-wide Security Plan

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Business Partners Systems Security Manual (BPSSM) defines entity-wide security plan controls as controls that "address the planning and management of an entity's control structure."

According to GAO FISCAM, key objectives of entity-wide security program planning and management are to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer related controls.

FISCAM states that "An entity-wide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures."

Comprehensive guidance on planning and managing an entity-wide security plan is contained in FISCAM Appendix VIII, titled "Principles for managing an information security program."

3.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-3 and E-4 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to the **development and implementation of an entity-wide security plan**. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-3. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-4.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-4 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to the development and implementation of an entity-wide security plan. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-7 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-7, the corresponding FISCAM control in Table E-6, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores

Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) include the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines around the **development and implementation of an entity-wide security plan.**

3.6 Periodic Review and Testing of Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be reassessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is controls around **access for application programmers to application data and source code.**

This guideline *shall*:

- Provide a high level understanding of controls around access for application programmers to application data and source code,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which directly concern **access for application programmers to application data and source code,** and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

4.2 Introduction to Access Controls for Application Programmers to Application Data and Source Code

(*Rev. 9, Issued:* 06-20-08, *Effective:* 07-01-08, *Implementation:* 07-22-08)

The Business Partners Systems Security Manual (BPSSM) defines application software development and change controls as controls that "address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information."

The GAO FISCAM states that "Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled."

A key component of comprehensive access controls for application programmers is 'Segregation of Duties'. FISCAM defines 'Segregation of duties' as controls that describe how work responsibilities should be segregated so that one person does not have access to or control over all of the critical stages of an information handling process. For instance; while a representative of the user community may initiate requests to changes in system capabilities, computer programmers should not be able to write, test, and approve program changes; and a user who has entered transactions in the system, should not have the capability to also review and approve the processing of all such transactions. Often, proper segregation of duties is achieved by splitting responsibilities between two or more organizational groups to ensure independence and objective checks and balances. These controls can be enforced through automated and/or manual measures.

4.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-9 and E-10 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to **application programmers' access to application data and source code**. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-9. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-10.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-10 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to **application programmers' access to application data and source cod**e. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-10 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-10, the corresponding FISCAM control in Table E-9, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines **around application programmers' access to application data and source code.**

4.6 **Periodic Review and Testing of Controls**

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be reassessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is **change management procedures.** Included in the controls around change management are requirements for maintaining change management documentation.

This guideline *shall*:

- Provide a high level understanding of change management procedures,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related **change management procedures**, and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

5.2 Introduction to Change Management Procedures

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Business Partners Systems Security Manual (BPSSM) defines application software development and change controls as controls that "address the modification and development of application software programs to ensure that only authorized software is utilized in the handling of Medicare and Federal Tax Information."

The GAO FISCAM states that:

"Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled."

"Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally, the application users have the primary responsibility for authorizing systems changes. However, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective. For this reason, an entity may require a senior systems developer to co-authorize a change."

"The use of standardized change request forms helps ensure that requests are clearly communicated and that all approvals are documented. Authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected."

5.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-12 and E-13 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to change management procedures. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-12. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-13.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-13 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to **change management procedures.** Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-13 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-13, the corresponding FISCAM control in Table E-12, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines around **change management procedures.**

5.6 Periodic Review and Testing of Controls

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems. Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be reassessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls is the **implementation and maintenance of security configuration templates.**

This guideline *shall*:

- Provide a high level understanding of **implementation and maintenance of** security configuration templates,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related to the **implementation and maintenance of security configuration templates**, and
- Provide a sample of prior instances of non-compliance with the above controls and recommended corrective measures.

6.2 Introduction to the Implementation and Maintenance of Security Configuration Templates

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Business Partners Systems Security Manual (BPSSM) and the GAO FISCAM define configuration management as "the control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system."

The BPSSM also states "The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires NIST to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal *g*overnment. The guidelines and checklists are developed to help system operators configure security within these systems to the highest level possible."

NIST has produced Special Publication 800-70 "Security Configuration Checklists Program for IT Products - Guidance for Checklist Users and Developers" to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products.

NIST also states that "a security configuration checklist" (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular operational environment. It could also include templates or automated scripts and other procedures. Checklists can be created by IT vendors for their own products or created by other organizations such as consortia,

academia, open source, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products."

6.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Security configuration templates take one of two forms. Some configuration templates are software-based in the form of a file or files which contain predetermined security settings which can be applied to single or multiple systems in an automated fashion. The other type of configuration template is policy-based and in the form of a checklist or recommendations guide, applied manually to the system during initial build and deployment.

Both NIST and the NSA provide security configuration checklists and security configuration guides for multiple operating systems and applications. Additionally, Security Technical Implementation Guides (STIGs) are published as tools to assist in the improvement of the security of Department of Defense (DOD) information systems. They are created using the principle that the most effective way to improve security in information systems is to include security in the initial design and development. As such, they provide the technical security policies, requirements, and implementation details for applying security concepts to information systems.

According to the BPSSM, CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program. Specifically, MACs and EDCs are required to start with these baseline configurations listed in the Security Technical Implementation Guides (STIGs) and document any exceptions based on environment-specific implementation. The use of STIGs *shall*:

- Reduce the likelihood of successful intrusions or attacks;
- Facilitate secure configuration of systems prior to network deployment;
- Assist with monitoring systems for on-going conformance with security configurations

Section 3.10.1 of this document (BPSSM) contains a list of applicable STIGs and their location.

Some operating system vendors include robust configuration management capabilities within the software. For example, Microsoft has included multiple methods to natively manage the configuration of Windows systems. The Windows Security Configuration Manager tool set allows administrators to create, apply and edit the security for local computers, organizational units, or domains. Windows also allows the construction and application of software-based security configuration templates. Microsoft states,

"With the Security Templates snap-in for Microsoft Management Console, administrators can create a security policy for computers or for networks. It is a single point of entry where the full range of system security can be taken into account. The Security Templates snap-in does not introduce new security parameters; it simply organizes all existing security attributes into one place to ease security administration."

The BPSSM states that "Business partners are **required** to perform an annual risk assessment in accordance with the CMS Information Security RA Methodology." The relevant FISCAM and NIST SP 800-53 controls identified to mitigate the risks discovered in the risk assessment can then be used to develop effective security configuration templates. Additionally, the BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-15 and E-16 list all the controls in FISCAM and NIST SP 800-53 respectively which are applicable to the **implementation and maintenance of security configuration templates**. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-15. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-16.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-16 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to the **implementation and maintenance of security configuration templates**. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier. Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-16 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-16, the corresponding FISCAM control in Table E-15, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines related to the **implementation and maintenance of security configuration templates**.

6.6 Periodic Review and Testing of Controls (*Rev. 9*, *Issued: 06-20-08*, *Effective: 07-01-08*, *Implementation: 07-22-08*)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems (which all CMS systems are

considered to be). Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls. Additionally, the BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

FISCAM refers to the maintenance of security configuration templates more specifically when it discusses maintaining System Security Plans. It states,

"To be effective, the policies and plan should be maintained to reflect current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the types and configuration of computer resources in use. Revisions to the plan should be reviewed, approved, and communicated to all employees. Outdated policies and plans not only reflect a lack of top management concern, but also may not address current risks and, therefore, may be ineffective."

The BPSSM states that "CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity." As requirements change or arise from the configuration management program, these new changes should be reflected by changes in the appropriate template.

7.1 Overview

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

A key component of effective information technology (IT) controls is security and a key foundation of comprehensive security controls includes a **Testing Process for the SANS Top 20 Internet Security Vulnerabilities**. This guideline *shall*:

- Provide a high level understanding of the SANS Top 20 Internet Security Vulnerabilities,
- Facilitate the identification of IT controls, in key *Federal* guidelines and standards, which are directly related to Testing for the SANS Top 20 Internet Security Vulnerabilities, and
- Provide a sample of prior instances of lack of identification and remediation of the SANS Top 20 Internet Security Vulnerabilities and recommended testing approaches.

7.2 Introduction to Testing for the SANS Top 20 Internet Security Vulnerabilities

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The GAO FISCAM states that an important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. To implement an effective security plan, top management should monitor its implementation and adjust the plan in accordance with changing risk factors. Over time, policies and procedures may become inadequate because of changes in operations or deterioration in the degree of compliance. Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan.

OMB Circular A-130, Appendix III, requires that *Federal* agencies review the security of their general support systems and major applications at least once every 3 years or sooner, if significant modifications have occurred or where the risk and magnitude of harm are high.

In addition, the Federal Managers Financial Integrity Act (FMFIA) of 1982 and OMB Circular A-123 require agencies to annually assess their internal controls, including computer-related controls, and report any identified material weaknesses to the President and the Congress.

When significant weaknesses are identified, the related risks should be reassessed, appropriate corrective actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. This is an important aspect of management's risk management responsibilities. In addition to modifying written policies to correct

identified problems, implementation of the corrective actions should be tested to see whether they are understood and are effective in addressing the problem. Management should continue to periodically review and test such corrective actions to see that they remain effective on a continuing basis.

The SANS (SysAdmin, Audit, Network, Security) Institute (or simply SANS) is one of the most trusted and largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center. SANS was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community.

The "Top Ten" list was first released by the SANS Institute and the National Infrastructure Protection Center (NIPC) in 2000. Today, though it is now called the Top Twenty, it covers over 230 well-known, often-exploited vulnerabilities in the Windows and UNIX environments. Thousands of organizations use the list to prioritize their efforts so they can close the most dangerous holes first. The majority of successful attacks on computer systems via the Internet can be traced to the exploitation of security flaws on this list. The SANS/FBI Top Twenty includes step-by-step instructions and pointers to additional information useful for correcting the flaws. SANS updates the list and the instructions as more critical threats and more current or convenient methods are identified.

The SANS Institute states that the SANS Top-20 2004 is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited elements in UNIX (SUN Solaris, IBM AIX, HP-UX, BSD, and Linux, etc.) environments. There are thousands of security incidents each year affecting these operating systems; however, the overwhelming majority of successful attacks target one or more of these twenty vulnerable services.

7.4 Specific Controls to be Implemented

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The SANS Top-20 list is a living document and is regularly updated. It includes step-bystep instructions and pointers to additional information useful for correcting common security flaws in Windows and UNIX operating systems. SANS updates the list and the instructions as more critical threats and more current or convenient methods of protection are identified. Table E-18 provides a list of the 20 vulnerable as described by the SANS Institution.

Top Vulnerabilities to Windows SystemsW1 - Web Servers & ServicesW2 - Workstation ServiceW3 - Windows Remote Access ServicesW4 - Microsoft SQL Server (MSSQL)W5 - Windows AuthenticationW6 - Web BrowsersW7 - File-Sharing ApplicationsW8 - LSAS ExposuresW9 - Mail ClientW10 - Instant MessagingTop Vulnerabilities to UNIX SystemsU1 - BIND Domain Name Service (DNS)U2 - Web ServerU3 - AuthenticationU4 - Version Control SystemsU5 - Mail Transport ServiceU6 - Simple Network Management Protocol (SNMP)U7 - Open Secure Sockets Layer (SSL)U8 - Misconfiguration of Enterprise Services NIS/NFSU9 - Databases
 W2 - Workstation Service W3 - Windows Remote Access Services W4 - Microsoft SQL Server (MSSQL) W5 - Windows Authentication W6 - Web Browsers W7 - File-Sharing Applications W8 - LSAS Exposures W9 - Mail Client W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 W3 - Windows Remote Access Services W4 - Microsoft SQL Server (MSSQL) W5 - Windows Authentication W6 - Web Browsers W7 - File-Sharing Applications W8 - LSAS Exposures W9 - Mail Client W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 W4 - Microsoft SQL Server (MSSQL) W5 - Windows Authentication W6 - Web Browsers W7 - File-Sharing Applications W8 - LSAS Exposures W9 - Mail Client W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 W5 - Windows Authentication W6 - Web Browsers W7 - File-Sharing Applications W8 - LSAS Exposures W9 - Mail Client W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 W6 - Web Browsers W7 - File-Sharing Applications W8 - LSAS Exposures W9 - Mail Client W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 W7 - File-Sharing Applications W8 - LSAS Exposures W9 - Mail Client W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 W8 - LSAS Exposures W9 - Mail Client W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 W9 - Mail Client W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 W10 - Instant Messaging Top Vulnerabilities to UNIX Systems U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
Top Vulnerabilities to UNIX SystemsU1 - BIND Domain Name Service (DNS)U2 - Web ServerU3 - AuthenticationU4 - Version Control SystemsU5 - Mail Transport ServiceU6 - Simple Network Management Protocol (SNMP)U7 - Open Secure Sockets Layer (SSL)U8 - Misconfiguration of Enterprise Services NIS/NFS
 U1 - BIND Domain Name Service (DNS) U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
 U2 - Web Server U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
U3 - Authentication U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
U4 - Version Control Systems U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
U5 - Mail Transport Service U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
U6 - Simple Network Management Protocol (SNMP) U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
U7 - Open Secure Sockets Layer (SSL) U8 - Misconfiguration of Enterprise Services NIS/NFS
U8 - Misconfiguration of Enterprise Services NIS/NFS
U9 - Databases
U10 - Kernel

 Table E-17. SANS Top 20 Internet Security Vulnerabilities (as of 10/08/04 – v. 5)

For each of the vulnerabilities, SANS lists on its website: description, operating system affected, related CVE entries, how to protect against the vulnerability, and how to test to determine if the vulnerability exists on a system. For the testing process for each vulnerability SANS indicates the manual process for testing (if any) as well as examples of automated tools (both open source and commercial) which can scan for the vulnerability.

NIST Special Publication 800-42, Guideline on Network Security Testing, identifies several different types of security testing and vulnerability monitoring. Some testing techniques are predominantly manual, requiring an individual to initiate and conduct the test. Other tests are highly automated and require less human involvement. Regardless of the type of testing, staff that setup and conduct security testing should have significant security and networking knowledge, including significant expertise in the following areas: network security, firewalls, intrusion detection systems, operating systems, programming and networking protocols (such as TCP/IP).

The following are types of testing techniques and tools:

- Network Scanning
- Vulnerability Scanning
- Password Cracking
- Log Review
- Integrity Checkers
- Virus Detection
- War Dialing
- War Driving (802.11 or wireless LAN testing)
- Penetration Testing

NIST SP 800-42 also references the SANS Top 20 Internet Security Vulnerabilities in its discussion and recommendations regarding security testing. NIST specifically states that the main focus of this document is the basic information about techniques and tools for individuals to begin a network security testing program. But it also states that this document is by no means all-inclusive. Individuals and organizations should consult the references provided in this document, such as the SANS list, as well as vendor product descriptions and other sources of information. And although the document is not all-inclusive, it is comprehensive in that it discusses how to implement security testing for vulnerabilities such as the SANS list while keeping a perspective of aligning with other security related practices for government information systems (such as the System Development Life Cycle and Certification and Accreditation processes).

The BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

All controls documented in the BPSSM are mandatory and *shall* be in place. It should be noted, however, that FISCAM and NIST SP 800-53 are viewed as 'guidance' and as such some controls may not apply to specific IT environments within CMS as long as clear and concise reasoning for the case is documented. Barring such exceptions, all controls are deemed applicable, **unless other compensatory controls are in place, which satisfy the control objective.**

Tables E-19 and E-20 list the controls in FISCAM and NIST SP 800-53 respectively which are applicable to **a Testing Process for the SANS Top 20 Internet Security Vulnerabilities**. Refer to Chapter Three (3) of FISCAM for the "Control Techniques" and "Audit Procedures" for each "Control Activity" in Table E-19. Refer to Appendix F (Security Control Catalogue) of NIST SP 800-53 for a more detailed discussion of each control in Table E-20.

The Federal Information Security Management Act of 2002 (FISMA) compliance guidance documented in NIST SP 800-53 recommends that each information system first be categorized as a low, moderate or high impact security category system using the approach documented in Federal Information Processing Standard (FIPS) number 199. Specific "Control Enhancements", within each control, are then to be implemented in accordance with this categorization. CMS management requires that Medicare Claims Processing Systems and Medicare Data Center systems be categorized as "high impact" security systems.

As mentioned above, Table E-20 contains a listing of all FISMA controls listed in Appendix F (Security Control Catalogue) of NIST SP 800-53 which are applicable to **Testing for the SANS Top 20 Internet Security Vulnerabilities**. Refer to NIST SP 800-53 for a description of each control and the applicable "Control Enhancements" for "High Control Baseline" (i.e., High Impact) systems. For ease of cross referencing to NIST SP 800-53, each control and control enhancement is preceded by the corresponding NIST SP 800-53 control identifier.

Refer to Appendix F of NIST SP 800-53 for "supplemental guidance" on each control listed in Table E-20 and to Appendix E of NIST SP 800-53 for a description of "Minimum Assurance Requirements" for High Baseline information systems.

In order to provide further detailed guidance on specific controls for each NIST control in Table E-20, the corresponding FISCAM control in Table E-19, if applicable, is identified. The reader can then refer to Chapter Three (3) of FISCAM for detailed guidance on "control techniques" and "audit procedures" for each of the corresponding FISCAM controls.

Within the BPSSM, CMS has outlined the mandatory Core Security Requirements (CSRs) which need to be in place in every information system that processes or stores Medicare-related data. Business partners *shall* establish and maintain adequate controls to ensure the confidentiality, integrity, and availability of Medicare data. There is a discussion of the CSRs within the body of the BPSSM and a detailed listing of all controls in Attachment A of the BPSSM. The CSRs are organized into categories, general requirements, control techniques, and protocols.

CMS management is committed to ensuring that each version of the BPSSM (current and future versions) includes the applicable FISCAM and NIST SP 800-53 controls discussed above in order to facilitate full compliance with guidelines related to **Testing for the SANS Top 20 Internet Security Vulnerabilities.**

7.6 **Periodic Review and Testing of Controls**

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Computers and the environments in which they operate are dynamic. Business process needs and the supporting technology, data sensitivity, information systems, risks associated with the systems and security requirements are ever-changing. Changes that can impact the security environment include: technological developments such as modifications to external network (and internet) connectivity; changes in the sensitivity or mission criticality of information; or the emergence of new internal and external threats. Authorized system users and operators, as well as unauthorized individuals internal and external to CMS, can discover new ways to bypass or subvert security. This environment continually introduces new vulnerabilities to system security. Strict adherence to existing procedures is not a given and the security procedures and controls become outdated over time.

Testing and monitoring of controls is a process to assess the effectiveness of internal controls performance over time. It involves assessing the compliance and operating effectiveness of existing controls and taking the necessary corrective actions on a timely basis. Every security control needs an assurance mechanism to ensure effectiveness. Refer to Appendix E of NIST Special Publication 800-53 for guidance on assurance mechanisms for high impact/criticality information systems (which all CMS systems are considered to be). Apart from regular testing and year-round monitoring of the effectiveness of existing controls, given the dynamic environment of information security, the design of the security controls *shall* be re-assessed and modified to reflect on-going operation and technological developments. Risk management is an integral part of the entire process of ensuring proper design of security controls and proper testing of existing controls.

Accordingly, the management practices, roles and responsibilities and specific security controls documented in the BPSSM *shall* be reviewed and modified on an on-going basis to ensure compliance with updates to *Federal* standards (such as FISCAM and FISMA compliance guidance) as well as developments in industry best practices.

Often, several of these testing techniques are used together to gain a more comprehensive assessment of the overall network security posture. For example, penetration testing usually includes network scanning and vulnerability scanning to identify vulnerable hosts and services that may be targeted for later penetration. Some vulnerability scanners incorporate password cracking. None of these tests by themselves will provide a complete picture of the network or its security posture.

NIST Special Publication 800-42 Guideline on Network Security Testing stresses the need for an effective security testing program within *Federal* agencies. Testing serves several purposes. One, no matter how well a given system may have been developed, the nature of today's complex systems with large volumes of code, complex internal interactions, interoperability with uncertain external components, unknown interdependencies coupled with vendor cost and schedule pressures, means that exploitable flaws will always be present or surface over time. Accordingly, security testing must fill the gap between the state of the art in system development and actual operation of these systems. Two, security testing is important for understanding, calibrating, and documenting the operational security posture of an organization. Aside from development of these systems, the operational and security demands must be met in a fast changing threat and vulnerability environment. Attempting to learn and repair the state of your security during a major attack is very expensive in cost and reputation, and is largely ineffective. Three, security testing is an essential component of improving the security posture of organizations. Organizations that have an organized, systematic, comprehensive, ongoing, and priority driven security testing regimen are in a much better position to make prudent investments to enhance the security posture of their systems.

The BPSSM requires that penetration testing be performed as needed and at least annually; and an Enterprise Security Posture Review be conducted at least quarterly.

8 References

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), January 1999.

OMB Guidance on FISMA Reporting Instructions, Memorandum for Heads of Executive Departments and Agencies, June 13, 2005.

Federal Information Security Management Act (FISMA) of 2002.

NIST Special Publication 800-53 *Revision 2*, Recommended Security Controls for Federal Information Systems, *December 2007*.

Appendix F: Security Configuration Management

Table of Contents

(Rev. 9, 06-20-08)

1 Introduction

2 Security Technical implementation Guides (STIG)

3 Department of Health and Human Services (*DHHS*) Minimum Security Configuration Standards

4 DHHS Federal Desktop Core Configuration (FDCC) Standard for Windows XP

1 Introduction

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) requires *the National Institute of Standards and Technology* (NIST) to develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal government.

2 Security Technical implementation Guides (STIG)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The guidelines, called STIGs, and checklists, called Security Checklists, are developed to help system operators configure security within their systems to the highest level possible. The STIGs and Security Checklists were formerly available at a NIST web page because the source Defense Information Systems Agency (DISA) web page was restricted to users in .gov and .mil domains. That restriction is no longer in effect, so NIST no longer hosts the DISA STIG and Security Checklist links.

The DISA *Web* page link for STIGs is: <u>http://iase.disa.mil/stigs/stig/index.html</u>, and for Security Checklists: <u>http://iase.disa.mil/stigs/checklist/index.html</u>. CMS recommends that business partner *Systems Security Officers* (SSO) (or their designated representative) subscribe to the DISA STIG-News Mailing List at: <u>http://iase.disa.mil/stigs/index.html</u> so they will be notified whenever updated or new STIGs become available.

The National Security Agency (NSA) has also developed and distributed configuration guidance for a wide variety of software from open-source to proprietary. The objective of the NSA configuration guidance program is to provide administrators with the best possible security options in the most widely used products. NSA provides these guidelines at: <u>http://www.nsa.gov/snac/downloads_all.cfm</u>.

The Center for Internet Security (CIS) provides security configuration benchmarks that represent a prudent level of due care, and are working to define consensus best-practice security configurations for computers connected to the Internet. CIS scoring tools analyze and report system compliance with the technical control settings in the benchmarks. The CIS benchmarks and scoring tools are available for download at: *http://www.cisecurity.com/benchmarks.html*.

The use of STIGs:

- Reduces the likelihood of successful intrusions or attacks;
- Facilitates secure configuration of systems prior to network deployment; and
- Assists with monitoring systems for on-going conformance with security configurations.

The latest versions of these documents can be obtained from the DISA web site by subscribing to the STIG-News Mailing List to receive update notifications.

3 Department of Health and Human Services Minimum Security Configuration Standards

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The Department of Health and Human Services (*D*HHS) is responsible for implementing and administering an information assurance and privacy program to protect its information resources, in compliance with applicable public laws, *F*ederal regulations, and Executive Orders, including the Federal Information Security Management Act of 2002 (FISMA); the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, dated November 28, 2000; and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The *D*HHS Minimum Security Configuration Standards were created as part of the *D*HHS Information Assurance and Privacy Program to supply standards for configuring Departmental Systems and Applications using Minimum Standard Configurations.

At a minimum, CMS expects *business partners to comply* with the *D*HHS configuration standards described below.

4 DHHS Federal Desktop Core Configuration (FDCC) Standard for Windows XP (Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The DHHS is responsible for implementing and administering an information security and privacy program to protect its information resources. The DHHS must be compliant with applicable public laws, Federal regulations, and Executive Orders, including FISMA; OMB Circular A-130, Management of Federal Information Resources, and HIPAA. To meet these requirements, DHHS instituted the DHHS Information Security Program Policy and the DHHS Information Security Program Handbook documents.

The DHHS developed the DHHS Federal Desktop Core Configuration (FDCC) Standard for Windows XP in response to OMB Memorandum (M)-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems, released on March 22, 2007. In collaboration with its Operating Divisions (OPDIVs), DHHS developed the standard by testing the original FDCC standard provided by NIST on July 31, 2007, and making appropriate adjustments to best suit the DHHS and its OPDIV's environment. The resulting DHHS FDCC Standard must be implemented at each OPDIV (i.e., CMS) and its contractor computers that are owned or operated by a contractor on behalf of, or for, the OPDIV, or are integrated into a Federal system subject to FDCC.

The DHHS considers the DHHS FDCC Standard for Windows XP document "sensitive" so it is not publicly available. To obtain a copy of the DHHS FDCC Standard, the designated Systems Security Officer (SSO) from each business partner must request a copy via the CISS Help Desk (<u>CISS@ngc.com</u>). CMS expects business partners to request a copy and comply with the DHHS FDCC Standard for Windows XP.

Appendix G: Acronyms and Abbreviations (Rev. 9, 06-20-08)

Α	
AAL	Authorized Access List
ABMAC	A/B Medicare Administrative Contractor
AC	Access Control
ACA	Annual Compliance Audit
ADM	Administrative
ADP	Automated Data Processing
AFE	Annual Frequency Estimate
AIE	Annual Impact Estimate
AIS	Automated Information System
AISSP	Automated Information Systems Security Program
ALE	Annual Loss Expectancy
ANSI	American National Standards Institute
APF	Authorized Program Facility
ARO	Annualized Rate of Occurrence
ARS	Acceptable Risk Safeguards
ASC	Accredited Standards Committee
AT	Awareness and Training
AU	Audit and Accountability

С

<u> </u>	
C&A	Certification and Accreditation
CA	Certification, Accreditation, and Security Assessments
CAP	Corrective Action Plan
CAST	Contractor Assessment Security Tool
ССМО	Consortium Contractor Management Officer
CD	Compact Disc
CD-ROM	Compact Disc-Read Only Memory
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIA	Confidentiality, Integrity, Availability
CICG	Critical Infrastructure Coordination Group
CIO	Chief Information Officer
CIS	Center for Internet Security
CISS	CMS Integrated Security Suite

CISSP	Certified Information Systems Security Professional
СМ	Configuration Management
СМР	Configuration Management Plan
CMS	Centers for Medicare and & Medicaid Services
СО	Central Office
СОВ	Coordination of Benefits
COMSEC	Communication Security
СР	Contingency Plan (or Planning)
CPIC	Certification Package for Internal Controls
CPU	Central Processing Unit
CSAT	Computer Security Awareness Training
CSIRC	Computer Security Incident Response Capability
CSR	Core Security Requirement
CVE	Common Vulnerability and Exposure
CWF	Common Working File

D

D	
DASD	Direct Access Storage Devices
DBA	Database Administrators
DBM	Database Management
DBMS	Database Management System
DC	Data Center (or District of Columbia)
DES	Data Encryption Standard
DHHS	Department of Health and Human ServicesSee HHS
DIR	Directed (by CMS)
DISA	Defense Investigative Security Agency
DMEMAC	Durable Medical Equipment Medicare Administrative Contractor
DNS	Domain Name System
DOS	Denial of Service
DSL	Digital Subscriber Line
DSS	Digital Signature Standard

E

EDC	Enterprise Data Center
EDI	Electronic Data Interchange
EDP	Electronic Data Processing
EF	Exposure Factor
E-mail	Electronic Mail
EO	Executive Orders
EVA	External Vulnerability Assessment

F	
FAR	Federal Acquisition Regulation
FE	FISMA Evaluation
FFS	Fee-for-Service
FIPS	Federal Information Processing Standards
FIS	Federal Information System Controls Audit Manual
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FMFIA	Federal Managers' Financial Integrity Act of 1982
FTI	Federal Tax Information (or Federal tax return information)
FY	Fiscal Year

Н

Н	High
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HISM	Handbook of Information Security Management
HITR	HCFA Information Technology Reference
HSPD	Homeland Security Presidential Directive

Ι

IA	Information Assurance (or Identification and Authentication)
IBM	International Business Machines (Corp.)
ID	Identification (or Identifier)
IDS	Intrusion Detection System
INFOSEC	Information Systems Security
IP	Internet Protocol
IR	Incident Response
IPL	Initial Program Load
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IRSAP	Internal Revenue Service Acquisition Procedure
IS	Information Security
ISSO	Information Systems Security Officer
IT	Information Technology
ITL	Information Technology Laboratory
ITMRA	Information Technology Management Reform Act

L	
L	Low

Μ

М	Moderate
MA	Major Application (or Maintenance)
MAC	Medicare Administrative Contractor
MBI	Minimum Background Investigation
MBSA	Microsoft Baseline Security Analyzer
МСМ	Medicare Carriers Manual
MCS	Multiple Console Support
MDCN	Medicare Data Communications Network
MIM	Medicare Intermediary Manual
MISPC	Minimum Interoperability Specification for PKI Components
MMA	Medicare Prescription Drug, Improvement, and Modernization Act of 2003
MP	Media Protection
MPS	Minimum Protection Standard
MVS	Multiple Virtual Storage

Ν

N	
<i>N/A</i>	Not Applicable
NARA	National Archives and Records Administration
NC	Network Computer
NCSC	National Computer Security Center
NIE	Net Impact Estimate
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NOS	Network Operating System
NSA	National Security Agency
NSC	National Security Council
NSTISSI	National Security Telecommunications and Information Systems Security Committee
NVA/ST	Network Vulnerability Assessment/Security Testing

0

OIG	Office of Inspector General
OIS	Office of Information Services (CMS)
OMB	Office of Management and Budget
ОРМ	Office of Personnel Management

OS	Operating System	
OTC	On-Time-Cost	

Р

<i>P.L</i> .	Public Law	
PartA	Part A Fiscal Intermediary	
PartB	Part B Carrier	
PC	Personal Computer	
PDA	Personal Digital Assistants	
PDD	Presidential Decision Directive	
PDS	Partitioned Data Sets	
PE	Physical and Environmental Protection	
PII	Personally Identifiable Information	
PIN	Personal Identification Number	
PISP	Policy for the Information Security Program	
PIV	Personal Identity Verification	
PKI	Public Key Infrastructure	
PL	Planning	
РМ	Project (Program) Managers	
РО	Project Officer	
РОА&М	Plan of Action and Milestones	
POC	Point-of-Contact	
PSC	Program Safeguard Contractor	
PSGH	CMS Policy Standards and Guidelines Handbook	
PS	Planning	
PSO	Physical Security Officer	
PUB	Publication	

Q

_ <u>v</u>	
QIC	Quality Integrity Contractor

R

RA	Risk Assessment
RAC	Recovery Audit Contractor
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFP	Requests for Proposals
RO	Regional Office
ROM	Read Only Memory

S		
SA	Security Administrator (or System and Services Acquisition)	
SAR	Safeguard Activity Report	
SAS	Statement on Auditing Standard	
SBI	Single Scope Background Investigation (SBI)	
SBU	Sensitive but unclassified	
SC	Security Category (or System and Communications Protection)	
SCHIP	State Children's Health Insurance Program	
SDLC	System Development Life Cycle	
SER	Scientific, Engineering, and Research	
SHS	Secure Hash Standard	
SI	System and Information Integrity	
SII	Security/Suitability Investigation Index	
SIRT	Security Incident Response Team	
SLE	Single Loss Expectancy	
SM	System Manager	
SMF	System Management Facility	
S-MIME	Secure Multi-purpose Internet Mail Extensions	
SOW	Statement of Work	
SP	Special Publication	
SPR	Safeguard Procedures Report	
SS	Standard System [Maintainer]	
SSA	Social Security Administration	
SSC	Systems Security Coordinator	
SSL	Secure Socket Layer	
SSM	Shared System Maintainers	
SSO	Systems Security Officer	
SSP	System Security Plan	
SSPM	System Security Plans Methodology	
SSSA	Senior Systems Security Advisor	
ST&E	Security Test and Evaluation	
STIG	Security Technical Implementation Guide	

Т

ТСР	Transmission Control Protocol	
TDES	Triple Data Encryption Algorithm	
TLS	Transport Layer Security	
ТО	Training Office	

U	
<i>U.S.C.</i>	United States Code
UID	User Identification
UL	Underwriter's Laboratory
	<u>, </u>

V	
VPN	Virtual Private Network

Ζ	
ZPIC	Zone Program Integrity Contractor

Appendix H: Glossary (*Rev. 9, 06-20-08*)

Term	Definition
Access	Ability to make use of any information system (IS) resource. (NIST SP 800-32)
Access Control	The process of granting or denying specific requests: (i) obtain and use information and related information processing services; and (ii) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances). (FIPS 201)
Access Control List	A list of entities that are authorized to have access to a
(ACL)	resource, together with their access methods.
Access Control Software	Software (CA-ACF2, RACF, CA-TOP SECRET), which is external to the operating system, provides a means of specifying
	who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection such as denying access for which the user is not expressly authorized, allowing access which is not expressly authorized but providing a wanting, or allowing access to all resources without warning regardless of authority. (FISCAM)
Account Management	Involves: (i) the process of requesting, establishing, issuing, and closing user accounts; (ii) tracking users and their respective access authorizations; and (iii) managing these functions. (NIST SP 800-12)
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non- repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (NIST SP 800-27A)

Accreditation	 (1) The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (FIPS 200) (2) The formal declaration by the DAA that a major application or general support system is granted approval to process using a prescribed set of safeguards in a specific operational environment. The accreditation decision is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate security after the implementation of an agreed upon set of security controls. (NIST SP 800-18)
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. (FIPS 200; OMB Circular A-130, App. III)
Adequately Met	Includes: (i) functionality that performs correctly, (ii) sufficient protection against unintentional errors (by users or software), and (iii) sufficient resistance to intentional penetration or by-pass. (NIST SP 800-27A)
Administrative Access	An advanced level of access to a computer or application that includes the ability to perform significant configuration changes to the computer's operating system. Also referred to as "privileged access" or "root access." (NIST SP 800-40)
Administrative Safeguards	Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. (NIST SP 800-66)
Advanced Encryption Standard (AES)	Specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. (NIST SP 800-46) Note: Through 2030, TDEA and AES will coexist as FIPS- approved algorithms, allowing for a gradual transition to AES.
AES	See Advanced Encryption Standard.
Alternate Site	An operating location other than the one at which an activity is usually performed for use by business functions when the primary facilities are unavailable.

Application	(1) The use of information resources (information and
	information technology) to satisfy a specific set of user
	requirements. (NIST SP 800-37)
	(2) Any data antime undata arrange an non-art more quart that
	(2) Any data entry, update, query, or report program that
	processes data for the user. (NIST SP 800-40)
Approved (Algorithm	FIPS approved or NIST recommended. An algorithm or
or Cryptography)	technique that is either:
	(i) specified in a FIPS or a NIST recommendation or
	(ii) adopted in a FIPS or NIST recommendation. (FIPS 201)
	There are only two (2) Approved encryption algorithms allowed
Amelitasturas	within CMS system environments: AES and Triple DES.
Architecture	A highly structured specification of an acceptable approach
	within a framework for solving a specific problem. An
	architecture contains descriptions of all the components of a
	selected, acceptable solution while allowing certain details of
	specific components to be variable to satisfy related constraints
	(e.g., costs, local environment, user acceptability). (FIPS 201)
Assessment Findings	Assessment results produced by the application of an
	assessment procedure to a security control or control
	enhancement to achieve an assessment objective; the execution
	of a determination statement within an assessment procedure by
	an assessor that results in either a satisfied or other than
	satisfied condition. (NIST SP 800-53A)
Assessment Method	A focused activity or action employed by an assessor for
	evaluating a particular attribute of a security control. (NIST SP
	800-37; NIST SP 800-53R1)
Assessment Procedure	A set of activities or actions employed by an assessor to
	determine the extent to which a security control is implemented
	correctly, operating as intended, and producing the desired
	outcome with respect to meeting the security requirements for
	the system. (NIST SP 800-37; NIST SP 800-53R1)
Asset	(1) A major application, general support system, high impact
	program, physical plant, mission critical system, or a logically
	related group of systems. (NIST SP 800-26)
	remieu group of systems. (14151 51 000-20)
	(2) Any software, data, hardware, administrative, physical
	communications, or personnel resource within an ADP system
	of activity.
	of activity.

Assurance	One of the five (5) "Security Goals." It involves support for our confidence that the other four (4) security goals (integrity, availability, confidentiality, and accountability) have been "adequately met" by a specific implementation. (NIST SP 800- 27A)
	Also see Adequately Met.
Attack	Attempt to gain unauthorized access to an IS's services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality. (CNSSI 4009)
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (<i>NIST SP 800-32;</i> CNSS <i>I 4009</i>)
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. (NIST SP 800-32)
Audit Reduction Tools	Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. (NIST SP 800-12)
Audit Trail	(1) A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period. (NIST SP 800-47)
	(2) Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. (CNSSI 4009)
Authenticate	<i>To confirm the identity of an entity when that identity is presented. (NIST SP 800-32)</i>
Authentication	(1) Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (FIPS 200)
	(2) Encompasses identity verification, message origin authentication, and message content authentication. (FIPS 190)
Authentication Mechanism	Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device. (NIST SP 800-72)

A sufference and a set	
Authorization	The official management decision given by a senior agency
	official to authorize operation of an information system and to
	explicitly accept the risk to agency operations (including
	mission, functions, image, or reputation), agency assets, or
	individuals, based on the implementation of an agreed-upon set
	of security controls. (NIST SP 800-37)
Authorizing Official	Official with the authority to formally assume responsibility for
	operating an information system at an acceptable level of risk
	to agency operations (including mission, functions, image, or
	reputation), agency assets, or individuals. Synonymous with
	Accreditation Authority. (FIPS 200)
Automated Labeling	Refers to labels employed on internal data structures (e.g.,
8	records, files) within the information system. (NIST SP 800-
	53R1)
Automated Marking	Refers to markings employed on external media (e.g., hardcopy
	documents output from the information system). The markings
	used in external marking are distinguished from the labels used
	on internal data structures described in automated labeling.
	(NIST SP 800-53R1)
Availability	<i>Ensuring timely and reliable access to and use of information.</i>
Avanuonny	(44 U.S.C., Sec. 3542)
Awareness	Activities which seek to focus an individual's attention on an
2111001011055	(information security) issue or set of issues. (NIST SP 800-50)
Background	<i>This is a more in-depth version of the LBI since the personal</i>
	investigation coverage is the most recent five (5) to seven (7)
Investigation (BI)	
	years. This investigation is required of those going into "high
Del	risk" public trust positions. (OPM)
Backup	A copy of files and programs made to facilitate recovery if
D 11	necessary. (CNSSI 4009)
Baseline	Includes information about a particular component's makeup
Configuration	(e.g., the standard software load for a workstation or notebook
	computer including updated patch information) and the
	component's logical placement within the information system
	architecture. Also includes a well-defined and documented
	specification to which the information system is built and
	deviations, if required, are documented in support of mission
	needs / objectives. (NIST SP 800-53R1)
Basic Input/Output	The program that starts up your computer and communicates
System (BIOS)	between the devices in your computer (such as your hard drive
	and graphics card) and the system.

Best Practices	The processes, practices, or systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency. (GAO Assessing Risks and Returns: A Guide for Evaluation Agencies' IT Investment Decision-making)
Biometric	A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics. (FIPS 201)
Boundary Protection	Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization and information systems not completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). (NIST SP 800-53R1)
Browsing	 (1) The act of electronically perusing files and records without authorization. (FISCAM) (2) The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (<i>CNSSI 4009</i>)
Business Continuity Plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. (NIST SP 800-34)
Business Impact Analysis (BIA)	An analysis of an IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (NIST SP 800-34)

Business Owner	(1) Official responsible for the overall procurement,
	development, integration, modification, or operation and maintenance of an information system. (NIST SP 800-53A)
	(2) Component or individual who have primary ownership of a major CMS business function or process. Examples are Medicare contractors, Program Safeguard Contractors, Shared Systems, Quality Improvement Organizations, Survey &
	Certification, Medicare Advantage Contractors, Medicare Call Centers, Enterprise Data Centers, and organizations conducting CMS sponsored research.
Business Recovery /Resumption Plan (BRP)	The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred. (NIST SP 800-34)
Certificate Policy	A specialized form of administrative policy tuned to electronic transactions performed during certificate management. It addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. (NIST SP 800-32)
Certification (Recertification)	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (FIPS 200)
Certification Agent	The individual, group, or organization responsible for conducting a security certification. (NIST SP 800-53R1)
Certification and Accreditation (C&A)	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

Certification	A trusted entity that issues and revokes public key certificates.
Authority (CA)	(FIPS 201)
Certification Practice Statement (CPS)	A statement of the practices that a Certification Authority employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services). (NIST SP 800-32)
Chain of Custody	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. (NIST SP 800-72)
Change Request	A request to modify any aspect of a system or environment including baseline requirements, hardware, or software.
Chief Information Officer (CIO)	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency [or organization] and other senior management personnel of the agency [or organization] to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency [or organization]; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency [or organization]; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency [or organization], including improvements to work processes of the agency [or organization]. (FIPS 200; P.L. 104- 106, Sec. 5125(b))
Clear	To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. (NIST SP 800-88)
Client (Application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server. (NIST SP 800-32)
Code	Instructions written in a computer programming language. (FISCAM)
	Also see Object Code and Source Code.

Cold Site	A backup facility that has the necessary electrical and physical
	components of a computer facility, but does not have the
	computer equipment in place. The site is ready to receive the
	necessary replacement computer equipment in the event that the
	user has to move from their main computing location to an
	alternate site. (NIST SP 800-34)
Collaborative	Applications and technology (e.g., whiteboarding, group
Computing	conferencing) that allow two or more individuals to share
	information real time in an inter- or intra-enterprise
	environment. (CNSSI 4009)
Common	A dictionary of common names for publicly known IT system
Vulnerabilities and	vulnerabilities. (NIST SP 800-51)
Exposures (CVE)	
Compensating	The management, operational, and technical controls (i.e.,
Security Control(s)	safeguards or countermeasures) employed by an organization
	in lieu of the recommended controls in the low, moderate, or
	high baselines described in NIST SP 800-53R1 (i.e., CSRs,
	ARS), that provide equivalent or comparable protection for an
	information system. (NIST SP 800-53R1)
Compromise	Disclosure of information to unauthorized persons, or a
	violation of the security policy of a system in which
	unauthorized intentional or unintentional disclosure,
	modification, destruction, or loss of an object may have
~ ~ .	occurred. (NIST SP 800-32)
Computer Forensics	The practice of gathering, retaining, and analyzing computer-
	related data for investigative purposes in a manner that
	maintains the integrity of the data. (NIST SP 800-61)
Computer Security	A violation or imminent threat of violation of computer security
Incident	policies, acceptable use policies, or standard computer security
a , a ,	practices. (NIST SP 800-61)
Computer Security	A capability set up for the purpose of assisting in responding to
Incident Response	computer security-related incidents; also called a Computer
Team (CSIRT)	Incident Response Team (CIRT) or a CIRC (Computer Incident
	<i>Response Center, Computer Incident Response Capability).</i> (NIST SP 800-61)
Confidentiality	Preserving authorized restrictions on information access and
	disclosure, including means for protecting personal privacy and
	proprietary information. (44 U.S.C., Sec. 3542)
Configuration	Process for controlling modifications to hardware, firmware,
Control	software, and documentation to protect the information system
	against improper modifications before, during, and after system
	implementation. (CNSSI 4009)
Console	Traditionally, a control unit such as a terminal through which a
	user <i>communicates</i> with a computer. In the mainframe
	environment, a <i>console</i> is the operator's station. (FISCAM)

Consortium	Currently consists of four (4) CMS offices (Northeastern,
Consortium	Southern, Midwestern, and Western) that oversee the operations
	at the Regional Offices.
Contingency Plan	Management policy and procedures designed to maintain or
(CP)	restore business operations, including computer operations,
	possibly at an alternate location, in the event of emergencies,
	system failures, or disaster. (<i>NIST SP 800-34</i>)
Contingency	See Contingency Plan.
Planning	
Continuity of	A predetermined set of instructions or procedures that describe
Operations Plan	how an organization's essential functions will be sustained for
(COOP)	up to thirty (30) days as a result of a disaster event before
	returning to normal operations. (NIST SP 800-34)
Control Techniques	Statements that provide a description of what physical,
1	software, procedural or people related condition <i>shall</i> be met or
	in existence in order to satisfy a core requirement.
Controlled Area	Any area or space for which the organization has confidence
	that the physical and procedural protections provided are
	sufficient to meet the requirements established for protecting
	the information and/or information system. (NIST SP 800-53A)
Cookie	A piece of information supplied by a Web server to a browser,
	along with requested resource, for the browser to store
	temporarily and return to the server on any subsequent visits or
	requests. (NIST SP 800-46)
Countermeasures	Actions, devices, procedures, techniques, or other measures
	that reduce the vulnerability of an information system.
	Synonymous with security controls and safeguards. (FIPS 200;
	CNSSI 4009)
Coverage	An attribute associated with an assessment method that
	addresses the scope or breadth of the assessment objects
	included in the assessment (e.g., types of objects to be assessed
	and the number of objects to be assessed by type). (NIST SP
	800-53A)
Credential	An object that authoritatively binds an identity (and optionally,
	additional attributes) to a token possessed and controlled by a
Credit Check	person. (NIST SP 800-63)
Creatt Cneck	This is an automated credit record search conducted through
	various major credit bureaus. It is included in most background
	investigations except the basic NACI investigation required of employees entering Non-Sensitive (Level 1) positions. (HHS
	Personnel Security/Suitability Handbook)
Critical Assets	Those physical and information assets required for the
CI IIICUI ASSEIS	performance of the site mission. (HHS IRM Policy)
Critical Infrastructure	Physical and cyber-based systems essential to the minimum
	operations of the economy and government. (PDD-63)
	operations of the economy and government. (FDD-03)

Cryptographic Algorithm A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. (FIPS 140-2) Cryptographic Key (Key) A parameter used in conjunction with a cryptographic algorithm that determines: The transformation of plaintext data into ciphertext data, The transformation of ciphertext data into ciphertext data, A digital signature computed from data, The verification of a digital signature computed from data, An authentication code computed from data, or An authentication code computed from data, or An authentication code computed from data, or An exchange agreement of a shared secret. (FIPS 140-3) Cryptographic Module The set of hardware and/or software that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. (NIST SP 800-32; FIPS 140-3) Cryptography The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. (NIST SP 800-21) Data Programs, files or other information stored in, or processed by, a computer system. (FIPS 112) Data Element A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. (NIST SP 800-47) Data Encryption The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67) The symmetric encryption algorithm that serves as the cryptographi	Criticality Level	Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level. (NIST SP 800-60)
(Key)algorithm that determines: 		inputs, including a cryptographic key, and produces an output.
Cryptographic ModuleThe set of hardware and/or software that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. (NIST SP 800-32; FIPS 140-3)CryptographyThe discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. (NIST SP 800-21)DataPrograms, files or other information stored in, or processed by, a computer system. (FIPS 112)Data ElementA basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. (NIST SP 800-47)Data Encryption Standard (DES)The symmetric encryption algorithm (TDEA). (NIST SP 800-67)Note: The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP 800-46)Data IntegrityThe property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (NIST SP 800-27A)		 algorithm that determines: The transformation of plaintext data into ciphertext data, The transformation of ciphertext data into plaintext data, A digital signature computed from data, The verification of a digital signature computed from data,
Modulesecurity functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. (NIST SP 800-32; FIPS 140-3)CryptographyThe discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. (NIST SP 800-21)DataPrograms, files or other information stored in, or processed by, a computer system. (FIPS 112)Data ElementA basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. (NIST SP 800-47)Data Encryption Algorithm (DEA)The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Data Encryption Standard (DES)The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special 		
CryptographyThe discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. (NIST SP 800-21)DataPrograms, files or other information stored in, or processed by, a computer system. (FIPS 112)Data ElementA basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. (NIST SP 800-47)Data Encryption Algorithm (DEA)The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Data Encryption Standard (DES)The symmetric encryption algorithm that serves as the cryptographic engine for the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Data IntegrityThe original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP 800-46)Data IntegrityThe property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (NIST SP 800-27A)		security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic
a computer system. (FIPS 112)Data ElementA basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. (NIST SP 800-47)Data Encryption Algorithm (DEA)The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Data Encryption Standard (DES)The symmetric encryption algorithm that serves as the cryptographic engine for the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Data IntegrityNote: The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP 800-46)Data IntegrityThe property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (NIST SP 800-27A)	Cryptography	The discipline that embodies principles, means and methods for providing information security, including confidentiality, data
Data ElementA basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. (NIST SP 800-47)Data Encryption Algorithm (DEA)The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Data Encryption Standard (DES)The symmetric encryption algorithm that serves as the cryptographic engine for the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Data IntegrityNote: The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP 800-46)Data IntegrityThe property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (NIST SP 800-27A)	Data	
Data Encryption Algorithm (DEA)The cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Data Encryption Standard (DES)The symmetric encryption algorithm that serves as the cryptographic engine for the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Note:The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP 800-46)Data IntegrityThe property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (NIST SP 800-27A)	Data Element	A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location. (NIST
Data Encryption Standard (DES)The symmetric encryption algorithm that serves as the cryptographic engine for the Triple Data Encryption Algorithm (TDEA). (NIST SP 800-67)Note: The original "single" DES algorithm is no longer secure because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP 800-46)Data IntegrityThe property that data has not been altered in an unauthorized 		
because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP 800-46)Data IntegrityThe property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (NIST SP 800-27A)	• =	cryptographic engine for the Triple Data Encryption Algorithm
manner. Data integrity covers data in storage, during processing, and while in transit. (NIST SP 800-27A)		because it is now possible to try every possible key with special purpose equipment or a high performance cluster. (NIST SP
	Data Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during
Data OwnerSee Information Owner.	Data Owner	See Information Owner.

Data Security	The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (FIPS 39)
	Also see Security Management Function.
Degauss	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors. (NIST SP 800-88)
Demilitarized Zone (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks. (NIST SP 800-41)
Denial of Service (DOS)	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) (NIST SP 800-27A)
Depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. (NIST SP 800-53A)
Destruction	The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive. (NIST SP 800- 88)
Digital Signature	 The result of a cryptographic transformation of data which, when properly implemented, provides the services of: Origin authentication, Data integrity, and Signer non-repudiation (FIPS 140-3)
Disaster Recovery Plan (<i>DRP</i>)	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. (NIST SP 800-34)
Discretionary Access Control	The basis of this kind of security is that an individual user, or program operating on the user's behalf is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. (FIPS 191)
Disposal	Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media. (NIST SP 800-88)

Diamention	An unplaneed quart that agains the second sector of sectors and
Disruption	An unplanned event that causes the general system or major
	application to be inoperable for an unacceptable length of time
	(e.g., minor or extended power outage, extended unavailable
	network, or equipment or facility damage or destruction). (NIST
	SP 800-34)
Distributed Denial of	A Denial of Service technique that uses numerous hosts to
Service (DDoS)	perform the attack. (NIST SP 800-61)
Domain	A set of subjects, their information objects, and a common
	security policy. (NIST SP 800-27A)
Electronic	The process of establishing confidence in user identities
Authentication (E-	electronically presented to an information system. (NIST SP
authentication)	800-63)
Electronic Mail	A store and forward method of composing, sending, storing,
(email)	and receiving messages over electronic communication systems.
	The term "email" (as a noun or verb) applies both to the
	Internet email system based on the Simple Mail Transfer
	Protocol (SMTP) and to X.400 systems, and to intranet systems
	allowing users within one organization to email each other.
	Often these workgroup collaboration organizations may use the
	Internet protocols or X.400 protocols for internal email service.
	Email is often used to deliver bulk unsolicited messages, or
	"spam", but filter programs exist which can automatically
	delete some or most of these, depending on the situation.
	(Wikipedia)
Electronic Media	(1) General term that refers to media on which data are
Lieunonii meaia	recorded via an electrically based process. (NIST SP 800-88)
	recorded via an electrically based process. (10151 51 600-66)
	(2) Electronic storage media including memory devices in
	computers (hard drives) and any removable /transportable
	digital memory medium, such as magnetic tape or disk, optical
	disk, or digital memory card; or
	Transmission media used to exchange information already in
	electronic storage media (e.g., Internet, extranet, leased lines,
	dial-up lines, private networks, and the physical movement of
	removable /transportable electronic storage media. (HIPAA)
Electronic Protected	Individually identifiable health information that is:
Health Information	(i) transmitted by electronic media, or
(EPHI)	(ii) maintained in electronic media. (HIPAA)

Electronic Signature	A symbol, generated through electronic means, that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria. (FISCAM)
Encryption	Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. (FIPS 185)
Entity	 (1) Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). (NIST SP 800-27A) (2) An individual (person), organization, device or process. (NIST SP 800-57, Part 1)
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. (FIPS 200; CNSSI 4009)
Event	Any observable occurrence in a network or system. (NIST SP 800-61)
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time. (NIST SP 800-53A)
External Information System (or Component)	An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (NIST SP 800-53A)
External Information System Service	An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). (NIST SP 800-53A)
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (NIST SP 800-53A)

Extranet	A virtual network created by connecting two intranets. An organization that connects remote locations with a VPN creates an extranet by linking its intranets together to form one virtual network. (NIST SP 800-41)
Federal Information System	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (40 U.S.C., Sec. 11331)
File	A collection of information logically grouped into a single entity and referenced by a unique name, such as a filename. (NIST SP 800-111)
General Support System(s) (GSS)	An interconnected set of information resources under the same direct management control which shares common functionality. <i>It</i> normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network. A departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. (<i>NIST SP</i> 800-53R1; OMB Circular A-130, <i>App. III</i>)
Guided Media	Medium in which a message flows through a physical media (e.g., twisted pair wire, coaxial cable, <i>optical fiber</i>) providing a closed path between sender and receiver. (Computer Assisted Technology Transfer Laboratory, Oklahoma State University)
Handled	(As in "Data handled.") Stored, processed or used in an ADP system or communicated, displayed, produced, or disseminated by an ADP system.
High-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. (FIPS 200)
Hot Site	A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster. (<i>NIST SP 800-34</i>)
Hotfix	Microsoft's term for a security patch. (NIST SP 800-40) Also see Patch.
<i>Identification</i>	 (1) The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. (NIST SP 800-47) (2) The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. (FIPS 201)

Identifier	A unique data string used as a key in the biometric system to name a person's identity and its associated attributes. (FIPS 201)
Identity	(1) A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person shall include sufficient additional information to make the complete name unique. (NIST SP 800-63)
	(2) The set of physical and behavioral characteristics by which an individual is uniquely recognizable. (FIPS 201)
Image	An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered. (NIST SP 800-72)
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (NIST SP 800-60, Vol. 2)
Inappropriate Usage	A person who violates acceptable computing use policies. (NIST SP 800-61)
Incident	(1) The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction.
	(2) An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (FIPS 200)
Incident Handling	The mitigation of violations of security policies and recommended practices. (NIST SP 800-61)
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT system(s). (NIST SP 800-34)
Incineration	A physically destructive method of sanitizing media; the act of burning completely to ashes. (NIST SP 800-88)
Incremental Backup	The process of making a copy of only the files that have changed since the last backup instead of backing up every file.

Independent	Any individual or group capable of conducting an impartial
Certification Agent or	assessment of an organizational information system.
Team	Impartiality implies that the assessors are free from any
	perceived or actual conflicts of interest with respect to the
	developmental, operational, and/or management chain of
	command associated with the information system or to the
	determination of security control effectiveness. Independent
	security certification services can be obtained from other
	elements within the organization or can be contracted to a
	public or private sector entity outside of the organization.
	Contracted certification services are considered independent if
	the information system owner is not directly involved in the
	contracting process or cannot unduly influence the
	independence of the certification agent or certification team
	conducting the assessment of the security controls in the
	information system. (NIST SP 800-53A)
Individual	(1) An assessment object that includes people applying
	specifications, mechanisms, or activities. (NIST SP 800-53A)
	(2) Person who is the subject of protected health information
	(PHI). (HIPAA)
Information	(1) An instance of an information type. (FIPS 200)
	(2) Any communication or reception of knowledge, such as
	facts, data, or opinions, including numerical, graphic, or
	narrative forms, whether oral or maintained in any other
	medium, including computerized databases, paper, microform,
	or magnetic tape. (OMB Circular A-130)
Information	Measures that protect and defend information and information
Assurance	systems by ensuring their availability, integrity, authentication,
	confidentiality, and non-repudiation. These measures include
	providing for restoration of information systems by
	incorporating protection, detection, and reaction capabilities.
	(CNSSI-4009)
Information Owner	Official with statutory or operational authority for specified
	information and responsibility for establishing the controls for
	its generation, collection, processing, dissemination, and
	disposal. (NIST SP 800-53R1; CNSSI 4009)

Information	Control of information system remnance, sometimes referred to
Remnance	as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user / role (or the actions of a process acting on behalf of a prior user / role) from being available to any current user/role (or current process) that obtains access to
	a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. (NIST SP 800-53R1)
Information Resource Owner	See <i>Business</i> Owner.
Information Resources	<i>Information and related resources, such as personnel, equipment, funds, and information technology. (44 U.S.C., Sec. 3502)</i>
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (44 U.S.C., Sec. 3542)
Information Security Agreement (ISA)	An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a memorandum of understanding or agreement (MOU/A) between the organizations. (NIST SP 800-26)
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. (CNSSI 4009)
Information Sharing	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C., Sec. 3502; OMB Circular A-130, App. III)
Information System	(1) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C., Sec. 3502
	(2) An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. (HIPAA)
Information System Owner (or Program Manager)	See Business Owner.

Information System Security Officer (ISSO)	(1) Individual responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with <i>System Security Officer</i>
	(SSO). (2) Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (NIST SP 800-53R1)
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures,
	services (including support services), and related resources. (40 U.S.C., Sec. 1401)
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. (FIPS 199)
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. (NIST SP 800- 32)
Integrity	(1) Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (44 U.S.C., Sec. 3542)
	(2) The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. (FIPS 140-2)

Interconnection	An agreement established between the organizations that own
Security Agreement	and operate connected IT systems to document the technical
(ISA)	requirements of the interconnection. The ISA also supports a
	Memorandum of Understanding or Agreement (MOU/A)
	between the organizations. (NIST SP 800-47)
Internet	When capitalized, the term "Internet" refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. (FISCAM)
Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time. (NIST SP 800-53A)
Intranet	A network internal to an organization but that runs the same protocols as the network external to the organization. Every organizational network that runs the TCP/IP protocol suite is an intranet. (NIST SP 800-41)
Intrusion Detection	Software that looks for suspicious activity and alerts
System (IDS)	administrators. (NIST SP 800-61)
Intrusion Prevention	System which can detect an intrusive activity and can also
System	attempt to stop the activity, ideally before it reaches its targets. (NIST SP 800-36)
IP Security (IPsec)	Request For Comments (RFC) 2411, protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol is used to negotiate the secret keys that protect Virtual Private Network (VPN) communications, and the level and type of security protections that will characterize the VPN. The most widely used key management protocol is the Internet Key Exchange (IKE) protocol. (NIST SP 800-46)
Key	See Cryptographic Key.
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. (FIPS 140-2)
Keystroke	The process used to view or record both the keystrokes entered
Monitoring	by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. (NIST SP 800-26)
Label	Information associated with a key that identifies the key's parameters attributes or intended use. (NIST SP 800-57, Part 1)
	Also see Security Label.

Least Privilege	The security objective of granting users only those accesses they
	need to perform their official duties. (NIST SP 800-12; NIST SP
I inited Deckensund	800-26) This investigation consists of a NACIC personal subject
Limited Background	This investigation consists of a NACI <i>C</i> , personal subject
Investigation (LBI)	interview, and personal interviews by an investigator of
	subject's background during the most recent three (3) years. (OPM)
Link Encryption	Link encryption encrypts all of the data along a
Link Encryption	communications path (e.g., a satellite link, telephone circuit, or
	<i>T1 line). Since link encryption also encrypts routing data,</i>
	communications nodes need to decrypt the data to continue
	routing. (NIST SP 800-12)
Local Access	Access to an organizational information system by a user (or an
	information system) communicating through an internal
	organization-controlled network (e.g., local area network) or
	directly to a device without the use of a network. (NIST SP 800-
	53A)
Log(s)	With respect to computer systems, to record an event or
	transaction. (FISCAM)
	Also see Record(s).
Low-Impact System	An information system in which all three security objectives
	(<i>i.e.</i> , confidentiality, integrity, and availability) are assigned a
	FIPS 199 potential impact value of low. (FIPS 200)
Major Application	An application that requires special attention to security due to
(MÅ)	the risk and magnitude of the harm resulting from the loss,
	misuse, or unauthorized access to or modification of the
	information in the application. Note: All Federal applications
	require some level of protection. Certain applications, because
	of the information in them, however, require special
	management oversight and should be treated as major.
	Adequate security for other applications should be provided by
	security of the systems in which they operate. (OMB Circular
	A-130, <i>App. III</i>)
	All "Major Applications" require "special management
	attention." The System Security Plan for a Major Application
	may be defined broadly enough to include hardware, software,
	networks, and even facilities where it is reasonable. This
	permits the systems to be bounded in reasonable ways for the
	purposes of security planning.
Malicious Code	Software or firmware intended to perform an unauthorized
	process that will have adverse impact on the confidentiality,
	integrity, or availability of an information system. A virus,
	worm, Trojan horse, or other code-based entity that infects a
	host. Spyware and some forms of adware are also examples of

	malicious code. (NIST SP 800-61; CNSSI 4009)
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (NIST SP 800-83)
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. (FIPS 200)
Mandatory Access Control	(1) A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. (NIST SP 800-44)
	(2) Access controls (which) are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information. (FIPS 191)
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system. (NIST SP 800- 53A)
Media	(1) Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large- Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (FIPS 200)
	(2) Includes both digital media (e.g., diskettes, magnetic tapes, external / removable hard drives, flash / thumb drives, compact disks [CD], digital video disks [DVD]) and non-digital media (e.g., paper, microfilm). (NIST SP 800-53R1)
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (NIST SP 800-88)
Medium	Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. (NIST SP 800-88)
Memorandum of Understanding /Agreement (MOU/A)	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (NIST SP 800-47)

Metrics	Tools designed to facilitate decision-making and improve
	performance and accountability through collection, analysis,
	and reporting of relevant performance-related data. (NIST SP
	800-55)
Minimum	This investigation includes a <i>NACIC</i> , a face-to-face personal
Background	interview between the investigator and the subject, and
Investigation (MBI)	telephone inquiries to selected employers. (OPM)
Mission Critical	Any telecommunications or information system that is defined
	as a national security system (i.e., FISMA) or processes any
	information the loss, misuse, disclosure, or unauthorized access
	to or modification of, would have a debilitating impact on the
	mission of an agency. (NIST SP 800-60, Vol. 2)
Mobile Code	Software programs or parts of programs obtained from remote
	information systems, transmitted across a network, and
	executed on a local information system without explicit
	installation or execution by the recipient. (NIST SP 800-53A)
Mobile Code	Software technologies that provide the mechanisms for the
Technologies	production and use of mobile code (e.g., Java, JavaScript,
	ActiveX, VBScript, PDF, Shockwave movies, Flash animations).
	(NIST SP 800-53A)
Moderate-Impact	An information system in which at least one security objective
System	(<i>i.e.</i> , confidentiality, integrity, or availability) is assigned a
	FIPS 199 potential impact value of moderate and no security
	objective is assigned a FIPS 199 potential impact value of high.
	(FIPS 200)
National Agency	An integral part of all background investigations, consisting of
Check (NAC)	searches of the OPM Security/Suitability Investigations Index
	(SII), the Defense Clearance and Investigations Index (DCII),
	the Federal Bureau of Investigation (FBI) Identification
	Division's name and fingerprint files, and other files or indices
	when necessary. (OPM)
National Agency	The basic and minimum investigation required on all new
Check and Inquiries	Federal employees consisting of a NAC with written inquiries
(NACI)	and searches of records covering specific areas of an
	individual's background during the past five (5) years (inquiries
	sent to current and past employers, schools attended,
	references, and local law enforcement authorities). (OPM)
National Agency	Includes the NACI with the addition of a credit record search.
Check and Inquiries	(OPM)
and Credit (NACIC)	
Need-To-Know	The necessity for access to, or knowledge or possession of,
	specific information required to carry out official duties.
	(CNSS <i>I 4009</i>)

Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the
	sender's identity, so neither can later deny having processed the information. (NIST SP 800-39)
Object	A passive entity that contains or receives information. (NIST SP 800-27A)
<i>Office of Information</i> <i>Systems (OIS)</i>	CMS office that ensures the effective management of CMS's information systems and resources. The office also develops and maintains central databases and statistical files, and directs Medicare claims payment systems.
Off-site Storage Facility	A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored for backup or other purposes.
Operating System (OS)	The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its principal component, the kernel, resides in memory at all times. The OS sets the standards for all application programs (such as the mail server) that run in the computer. The applications communicate with the OS for most user interface and file management operations. (NIST SP 800- 45)
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). (FIPS 200)
Organization	A federal agency or, as appropriate, any of its operational elements. (FIPS 200)
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. (NIST SP 800-32)
Overwrite	Writing patterns of data on top of the data stored on a magnetic medium. NSA has researched that one overwrite is good enough to sanitize most drives. (NIST SP 800-88)
Password	 (1) A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. (NIST SP 800-63) (2) A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. (FIPS 181)
	(3) A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. (FIPS 140-3)
Patch	An additional piece of code developed to address a problem in an existing piece of software. (NIST SP 800-40)

Penetration	Unauthorized act of bypassing the security mechanisms of a system. (CNSSI 4009)
Penetration Test	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. (NIST SP 800-53A)
Personal Identification Number (PIN)	A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits. (FIPS 201)
Personal Identity Verification Card (PIV Card)	Physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). (FIPS 201)
Personally Identifiable Information (PII)	Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual.
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. (NIST SP 800-83)
Physical Destruction	A sanitization method for optical media, such as CDs. (NIST SP 800-88)
Plaintext	Intelligible data that has meaning and can be understood without the application of decryption. (NIST SP 800-21)
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (OMB M-02-01)
Policy	An official statement of a position, plan or course of action established by an identified sponsoring authority, which is designed to influence, to provide direction and to determine decisions and actions with regard to a specific topic. Policies provide broad direction or goals. Standards, procedures and guidelines flow from policies. Also see Security Policy.

Portable and Mobile	Includes notebook computers, personal digital assistants,
Devices	cellular telephones; and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations. (NIST SP 800-53R1)
Position Sensitivity	The degree of risk and level of relative importance assigned to a specific position. (HHS Personnel Security/Suitability Handbook)
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a serious adverse effect (FIPS 199 moderate); or
	 (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. (NIST SP 800-39, FIPS 199 Adapted)
Privacy Impact	An analysis of how information is handled:
Assessment (PIA)	(<i>i</i>) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
	(ii) to determine the risks and effects of collecting, maintaining
	and disseminating information in identifiable form in an
	electronic information system, and
	(iii) to examine and evaluate protections and alternative
	processes for handling information to mitigate potential privacy risks. (NIST SP 800-60, OMB M-03-22)
Privacy Information	The individual's right to privacy must be protected in Federal
	Government information activities involving personal
	information. Such information is to be collected, maintained,
	and protected so as to preclude intrusion into the privacy of
	individuals and the unwarranted disclosure of personal
	information. (OMB Circular A-130)
Privileged Accounts	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network
	administrative accounts. (NIST SP 800-12)
Privileged Function	A function executed on an information system involving the
	control, monitoring, or administration of the system. (NIST SP
	800-53A)
Privileged User	Individual who has access to system control, monitoring, or
	administration functions (e.g., system administrator,
	information system security officer, maintainer, system
Procedures	programmer). (CNSSI 4009)(1) A course of action to be taken to perform a given task.
	(2) A mentionlaw weeks down avoid the first state of the literation
	(2) A particular method or guidance for implementing a policy
	or performing a task or operation which has to be executed in the same manner in order to always obtain the same result in
	the same manner in order to always obtain the same result in the same circumstance (e.g., emergency procedure). (Internet)
	ine same circumstance (e.g., emergency procedure). (Internet)

Production Programs	Programs that are being used and executed to support
	authorized organizational operations. Such programs are
	distinguished from "test" programs that are being developed or
	modified, but have not yet been authorized for use by
	management. (FISCAM)
Profile	A set of rules that describes the nature and extent of access to
	available resources for a user or a group of users with similar
	duties, such as accounts payable clerks. (FISCAM)
	Also see Standard Profile and User Profile.
Protected Health	Individually identifiable health information that is:
Information (PHI)	<i>(i) transmitted by electronic media,</i>
	(ii) maintained in electronic media, or
	<i>(iii) transmitted or maintained in any other form or medium.</i>
	(HIPAA)
	NOTE: PHI excludes individually identifiable health
	information in employment records held by a covered HIPAA
	entity in its role as employer.
Proxy	A proxy is an application that "breaks" the connection between
5	client and server. The proxy accepts certain types of traffic
	entering or leaving a network and processes it and forwards it.
	This effectively closes the straight path between the internal and
	external networks. Making it more difficult for an attacker to
	obtain internal addresses and other details of the organization's
	internal network. Proxy servers are available for common
	Internet services; for example, an Hyper Text Transfer Protocol
	(HTTP) proxy used for Web access, and an Simple Mail
	Transfer Protocol (SMTP) proxy used for e-mail. (NIST SP 800-
	44)
Public Information	Any information, regardless of form or format that an agency
r ubuc information	
	discloses, disseminates, or makes available to the public. (NIST $SP = 200.60$ MeV 2)
Dull's Kan Cartifiants	SP 800-60, Vol. 2)
Public Key Certificate	(1) A digital document issued and digitally signed by the private
	key of a Certification Authority that binds the name of a
	subscriber to a public key. The certificate indicates that the
	subscriber identified in the certificate has sole control and
	access to the private key. (NIST SP 800-63)
	(2) A set of data that contains a unique identifier associated
	with an entity, contains the public key associated withy the
	identifier, and is digitally signed by a trusted party, thereby
	binding the public key to the identifier. (FIPS 140-3)

Public Key	An architecture which is used to bind public keys to entities,
-	• •
Infrastructure (PKI)	enable other entities to verify public key bindings, revoke such
	bindings, and provide other services critical to managing public
	keys. (FIPS 196)
Pulverization	A physically destructive method of sanitizing media; the act of
	grinding to a powder or dust. (NIST SP 800-88)
Purge	Rendering sanitized data unrecoverable by laboratory attack
	methods. (NIST SP 800-88)
Quality Assurance	The function that reviews software project activities and tests
	software products throughout the software life-cycle to
	determine if:
	(<i>i</i>) the software project is adhering to its established plans,
	standards, and procedures, and
	(<i>ii</i>) the software meets the functional specifications defined by
	the user. (FISCAM)
Record(s)	(1) The recordings (automated and/or manual) of evidence of
	activities performed or results achieved (e.g., forms, reports,
	test results), which serve as a basis for verifying that the
	organization and the information system are performing as
	intended. Also used to refer to units of related data fields (i.e.,
	groups of data fields that can be accessed by a program and
	that contain the complete set of information on particular
	items). (FIPS 200)
	(2) A unit of related data fields. The group of data fields that
	can be accessed by a program and contains the complete set of
	information on a particular item. (FISCAM)
Recovery Procedures	Actions necessary to restore data files of an information system
	and computational capability after a system failure. (CNSSI
	4009)
Remanence	Residual information remaining on storage media after
	clearing. (NIST SP 800-88)
Remediation	<i>The act of correcting a vulnerability or eliminating a threat.</i>
	Three possible types of remediation are installing a patch,
	adjusting configuration settings, and uninstalling a software
	application. (NIST SP 800-40)
Remote Access	Access to an organizational information system by a user (or an
Kennote Meeebs	information system) communicating through an external, non-
	organization-controlled network (e.g., the Internet). Examples
	of remote access methods include dial-up, broadband, and wireless (NIST SP 800 52P1)
Demoste M. 1. (wireless. (NIST SP 800-53R1)
Remote Maintenance	Maintenance and diagnostic activities conducted by individuals
	communicating through an external, non-organization-
	controlled network (e.g., the Internet). (NIST SP 800-53A)

Remote Session	A session initiated whenever an organizational information
	system is accessed by a user (or an information system) communicating through an external, non-organization-
	controlled network (e.g., the Internet). (NIST SP 800-53R1)
Residual Risk	The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat. (NIST SP 800-33)
Residue	Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place. (NIST SP 800-88)
Resource	See Information Resource.
Resource Owner	See <i>Business</i> Owner.
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (FIPS 200 Adapted)
Risk Analysis	(1) The identification and study of the vulnerability of a system and the possible threats to its security. (FIPS 11-3)
	(2) The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. (NIST SP 800-27A)
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in-place security controls. (NIST SP 800-30 Adapted)
Risk Management	(1) A management approach designed to reduce risks inherent to system development and operations. (FISCAM)
	 (2) The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (FIPS 200 Adapted)

Risk Mitigation	Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. (NIST SP 800- 30)
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result. (NIST SP 800-32)
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. (FIPS 200)
Sanitize (or Sanitization)	Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. (NIST SP 800-88)
Scenario	A functional exercise staff member who simulates or represents non-participating individuals or organizations whose input or participation is necessary to the flow of the exercise. (NIST SP 800-84)
Secure Name /	Enables remote clients to obtain origin authentication and
Address Resolution Service (Authoritative	integrity verification assurances for the name / address resolution information obtained through the service. A domain
Source)	name system (DNS) server is an example of an information system that provides name / address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure DNS deployment. (NIST SP 800-53R1)
Secure Name / Address Resolution Service (Recursive or	An information system that provides name / address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST SP 800-81 provides
Caching Resolver)	guidance on secure domain name system deployment. (NIST SP 800-53R1]
Secure Sockets Layer (SSL)	Protocol based on public key cryptography. Used to generate a cryptographic session that is private to a Web server and a client browser. (NIST SP 800-41)
Security Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37)

Security Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (NIST SP 800-53A)
Security Attribute	A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes. (FIPS 188)
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. (FIPS 199; FIPS 200)
Security Certification	A formal testing of the security safeguards implemented in the computer system to determine whether they meet applicable requirements and specifications. To provide more reliable technical information, certification is often performed by an independent reviewer, rather than by the people who designed the system. (NIST <i>SP</i> 800-12)
Security Communications Protocol	A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection. (NIST SP 800-57)
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. (FIPS 200)
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. (NIST SP 800-53A)
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (FIPS 199; FIPS 200)
Security Domain	 (1) A set of subjects, their information objects, and a common security policy. (NIST SP 800-27A) (2) A collection of entities to which applies a single security policy executed by a single authority (EIDS 188).
Security Functions	policy executed by a single authority. (FIPS 188) The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based. (NIST SP 800-53A)

Security Impact	The analysis conducted by an agency official, often during the
Analysis	continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of
	the system. (NIST SP 800-37)
Security Incident	A security incident is a violation, or an imminent threat of a violation, of an explicit or implied security policy, acceptable use policies, or standard security practices.
	Also see Incident.
Security Label	<i>Explicit or implicit marking of a data structure or output media</i> <i>associated with an information system representing the FIPS</i> <i>199 security category, or distribution limitations or handling</i> <i>caveats of the information contained therein. (NIST SP 800- 53A)</i>
Security Level	A hierarchical indicator of the degree of sensitivity to a certain threat. It implies, according to the security policy being enforced, a specific level of protection. (FIPS 188)
Security Objective	Confidentiality, integrity, or availability. (FIPS 199; FIPS 200)
Security Plan	See System Security Plan (SSP).
Security Policy	 (1) A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance. (Federal IT Security Assessment Framework) (2) A set of writerin for the environment of accurity assessment for the security of accurity and the security for the security of accurity for the security for th
	(2) A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. (FIPS 188)
Security Requirements	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. (FIPS 200)
Security	Description of the minimum requirements necessary for an
Requirements Baseline	information system to maintain an acceptable level of security. (CNSS <i>I 4009</i>)
Security Service	 (1) A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication. (NIST SP 800-27A) (2) Mechanism used to provide confidentiality, data integrity, data integrity, and authentication.
	<i>authentication or non-repudiation of information. (NIST SP 800-57, Part 1)</i>

Security Test and	An examination and analysis of the security safeguards of a
Security Test and Evaluation (ST & E)	An examination and analysis of the security safeguards of a
Evaluation (ST&E)	system as they have been applied in an operational environment
Constant Touting	in order to determine the security posture of the system.
Security Testing	A process that is used to determine that the security features of
	a system are implemented and functioning as designed. This
	process includes hands on functional testing, penetration testing
	and verification.
Sensitive Information	(1) Any information whose loss, misuse, unauthorized access,
	unauthorized disclosure, or improper modification could
	adversely affect the national interest, the conduct of Federal
	programs, or the privacy to which individuals are entitled under
	the Privacy Act. (FISCAM)
	(2) Information that requires protection due to the risk and
	magnitude of loss or harm that could result from inadvertent or
	deliberate disclosure, alteration, or destruction of the
	•
	information. The term includes information whose improper use
	or disclosure could adversely affect the ability of an agency to
	accomplish its mission, proprietary information, records about
	individuals requiring protection under the Privacy Act, and
	information not releasable under the Freedom of Information
	Act. (NIST SP 800-26)
	(3) CMS Sensitive Information corresponds to <i>a</i> "High" <i>system</i>
	security level as described in section 4.0 of this document.
Sensitivity Levels	A graduated system of marking (e.g., low, moderate, high)
	information and information processing systems based on
	threats and risks that result if a threat is successfully conducted.
	(FIPS 201)
Separation of Duties /	To ensure that no single person has control of a transaction
Segregation of Duties	from beginning to end and that two or more people are
Segregation of Dances	responsible for its execution. This is intended to prevent one
	person from manipulating transactions for personal gain.
Service <i>C</i> ontinuity	This type of control involves ensuring that when unexpected
Controls	events occur, critical operations continue without interruption or
	are promptly resumed and critical and sensitive data are
	protected. (FISCAM)
Session	A session is an encounter between an end-user interface device
JUSSIUII	(e.g., computer, terminal, process) and an application,
	including a network logon. One user session is the time
	between starting the application and quitting. (Multiple
Canaian Canton 1	sources)
Session Control	The application of security mechanisms to network connections
	which are intended to prevent unauthorized persons from
	capturing or modifying network connection data, or taking
	control of pre-established network connections.

Shred	A method of sanitizing media; the act of cutting or tearing into
Shreu	small particles. (NIST SP 800-88)
Signature	A recognizable, distinguishing pattern associated with an
Jighalare	attack, such as a binary string in a virus or a particular set of
	keystrokes used to gain unauthorized access to a system. (NIST
	SP 800-61)
Signed Data	Data on which a digital signature is generated. (FIPS 196)
Significant Change	A physical, administrative, or technical modification that alters
Significant Change	the degree of protection required. <i>Examples include, but are not</i>
	limited to, changes in operating systems, computer hardware,
	firmware, operational environment, or system boundaries; new
	services or applications; or other conditions that potentially
	impact the system's security posture or accreditation status.
	(NIST SP 800-53R1)
Smart Card	A credit card with a built-in microprocessor and memory that is
	used for identification or financial transactions. When inserted
	into a reader, the card transfers data to and from a central
	computer. A smart card is more secure than a magnetic stripe
	card and can be programmed to self-destruct if the wrong
	password is entered too many times. (NIST SP 800-48)
Sniffer	Software that observes and records network traffic. (NIST SP
Shire	800-61) Synonymous with packet sniffer.
Social Engineering	An attempt to trick someone into revealing information (e.g., a
Social Engineering	password) that can be used to attack systems or networks.
	(<i>NIST SP 800-61</i>)
Special Management	Some systems require "special management attention" to
Attention	security due to the risk and magnitude of the harm that would
	result from the loss, misuse, unauthorized access to, or
	modification of the information in the system. (OMB Circular
	A-130)
Specification	An assessment object that includes document-based artifacts
	(e.g., policies, procedures, plans, system security requirements,
	functional specifications, and architectural designs) associated
	with an information system. (NIST SP 800-53A)
Spyware	Software that is secretly or surreptitiously installed into an
	information system to gather information on individuals or
	organizations without their knowledge; a type of malicious
	<i>code.</i> (<i>NIST SP 800-53A</i>)
Standard	A published statement on a topic specifying characteristics,
	usually measurable, that shall be satisfied or achieved in order
	to comply with the standard. (FIPS 201)
Storage	Retrievable retention of data. Electronic, electrostatic, or
	electrical hardware or other elements (media) into which data
	may be entered, and from which data may be retrieved. (NIST
	SP 800-88)

Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions. (NIST SP 800-18)
Suitability	Refers to identifiable character traits and conduct sufficient to decide whether an individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate integrity, efficiency, and effectiveness. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, and skills. (OPM)
System	(1) An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. (OMB Circular A-130)
	(2) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (NIST SP 800-53R1)
	A system normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people. A system's hardware may include mainframe systems, desktop systems (e.g., PC's, Macintoshes, laptops, handheld devices), workstations and servers (e.g., Unix, NT, NC), local area networks (LAN), and any other platform regardless of the operating system.
	Also see Information System.
System Administrator	A person who manages the technical aspects of a system. (NIST SP 800v2)
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (NIST SP 800- 34)
System Integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. (NIST SP 800-27A)
System Interconnection	The direct connection of two or more IT systems for the purpose of sharing data and other information resources. (NIST SP 800- 26)

System Interconnection	The direct connection of two or more IT systems for the purpose of sharing data and other information resources. (NIST SP 800- 47)
System Maintainer	The individual or group of individuals who have the responsibilities of continued maintenance (e.g. bug fixing, minor modifications /enhancements, performance tuning, and/or customer service) of an implemented system. A system maintainer may or may not also serve as the system developer for a given project.
System Media	Includes both digital media (e.g., diskettes, magnetic tapes, external / removable hard drives, flash / thumb drives, compact disks [CD], digital video disks [DVD]) and non-digital media (e.g., paper, microfilm). (NIST SP 800-53R1)
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (NIST SP 800-18; FIPS 200)
System Software	The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data. (FIPS 140-2)
System Test	A test performed on a complete system to evaluate its compliance with specified requirements. (NIST SP 800-84)
Tabletop Exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. (NIST SP 800-84)
Tailoring	The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed. (NIST SP 800-53A)
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. (FIPS 200)

Telecommunications	The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received. (NIST SP 800-60, Vol. 2)
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time. (NIST SP 800-53A)
Test Bed	<i>Test environment containing the software, data, and simulations necessary for testing systems.</i>
Test Plan	A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step. (NIST SP 800-84)
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (FIPS 200)
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment. (NIST SP 800-27A)
Threat Assessment	Formal description and evaluation of threat to an information system. (CNSSI 4009)
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent. (FIPS 200)
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity. (NIST SP 800-63)

Transport Layer	A protocol created to provide authentication, confidentiality
Security (TLS)	<i>A protocol created to provide dumentication, confidentiality</i> and data integrity between two communicating applications over the Internet. Although based on the precursor protocol SSL 3.0, TLS is considered an improvement to SSL 3.0. (Adapted from NIST SP 800-52)
	Note: While SSL 3.0 is the most secure of the SSL protocol versions, it is not approved for use in the protection of Federal information because it relies in part on the use of cryptographic algorithms that are not FIPS-approved. TLS, when properly configured, is approved for the protection of Federal information. (NIST SP 800-52)
Triple Data	An implementation of the Data Encryption Standard (DES)
<i>Encryption Algorithm</i> (<i>TDEA</i>) (a.k.a. <i>Triple</i> <i>DES</i>)	algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is
	less secure than AES. (NIST SP 800-46)
	Note: Through the year 2030, TDEA and AES will coexist as FIPS-approved algorithms-thus, allowing for a gradual transition to AES.
	Also and Triple Data Enormation Standard
Triple Data	Also see Triple Data Encryption Standard. Triple DES (i.e., TDEA) is recognized as the only FIPS-
Encryption Standard	approved DES algorithm. Other implementations of the DES
(Triple DES)	function are no longer authorized for protection of Federal government information. (NIST SP 800-67)
	Note: Through the year 2030, TDEA and AES will coexist as FIPS-approved algorithms-thus, allowing for a gradual transition to AES.
Trojan Horse	A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose. (NIST SP 800-61)
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the
	information system with the necessary confidence to support the
	system security policy. This mechanism can be activated only by the user or the security functions of the information system and
	the user or the security functions of the information system and cannot be imitated by untrusted software. (NIST SP 800-53A)
Two-factor	A type of authentication that requires two independent methods
Authentication	to establish identity and authorization to perform services. The
	three most recognized factors are:
	• "Something you are" (e.g., biometrics)
	• "Something you know" (e.g., password)
	• "Something you have" (e.g., smart card) (FIPS 140-3)

Unauthorized Access	Occurs when a user, legitimate or unauthorized, accesses a
	resource that the user is not permitted to use. (FIPS 191)
Unauthorized	An event involving the exposure of information to entities not
Disclosure	authorized access to the information. (NIST SP 800-57)
Unclassified	Information that has not been determined pursuant to E.O.
	12958 or any predecessor order to require protection against
	unauthorized disclosure and that is not designated as classified.
	(CNSS <i>I 4009</i>)
User	(1) Individual or (system) process authorized to access an
	information system. (CNSSI 4009)
	(2) Any organizational or programmatic entity that [utilizes or]
	receives service from an [automated information system]
	facility. A user may be either internal or external to the agency
	organization responsible for the facility, but normally does not
	report to either the manager or director of the facility or to the
	same immediate supervisor. (OMB Circular A-130)
Validation	The process of demonstrating that the system under
	consideration meets in all respects the specification of that
	system. (FIPS 201)
Virtual Private	(1) A virtual private network is a logical network that is
Network (VPN)	established, at the application layer of the Open Systems
	Interconnection (OSI) model, over an existing physical network
	and typically does not include every node present on the
	physical network. (NIST SP 800-46)
	(2) A virtual network, built on top of existing physical networks,
	which can provide a secure communications mechanism for
	data and other information transmitted between networks.
	(<i>NIST SP 800-113</i>)
Virus	A self-replicating program that runs and spreads by modifying
	other programs or files (NIST SP 800-61)
Vulnerability	Weakness in an information system, system security procedures,
	internal controls, or implementation that could be exploited or
	triggered by a threat source. (FIPS 200)
Vulnerability	Formal description and evaluation of the vulnerabilities in an
Assessment	information system. (CNSSI 4009
Warning Banner	A notice presented prior to authentication to a access-restricted
	system identifying the system as a non-public resource, warning
	that unauthorized access can result in legal persecution and
	stating that only authorized users are permitted to access the
****	system.
Wired Equivalent	Wired Equivalent Privacy, a security protocol for wireless local
Privacy (WEP)	area networks (WLANs) defined in the 802.11b standard. WEP
	was intended to provide the same level of security as that of a
	wired LAN. (NIST SP 800-46)

Wireless Application	A standard for providing cellular telephones, pagers, and other
Protocol (WAP)	handheld devices with secure access to e-mail and text-based
	Web pages. (NIST 800-48)
Workstation	An electronic computing device, for example, a laptop or
	desktop computer, or any other device that performs similar
	functions, and electronic media stored in its immediate
	environment. (HIPAA)
Worm	A self-replicating, self-propagating, self-contained program
	that uses networking mechanisms to spread itself. (NIST SP
	800-61)
Write	Fundamental operation in an information system that results
	only in the flow of information from a subject to an object.
	(CNSS <i>I 4009</i>)
Write Access	Permission to write to an object in an information system.
	(CNSS <i>I 4009</i>)
X.509 Certificate	The International Organization for
	Standardization/International Telecommunication Union –
	Standardization Department (ISO/ITU-T) X.509 standard
	defined two types of certificates – the X.509 public key
	certificate, and the X.509 attribute certificate. Most commonly
	(including this document), an X.509 certificate refers to the
	X.509 public key certificate. (NIST SP 800-57)
Zeroization	A method of erasing electronically stored data and
	cryptographic keys by altering or deleting the contents of the
	data storage to prevent recovery of the data. (Adapted from
	FIPS 140-2)