| CMS Manual System | **Department of Health & Human Services (DHHS)** |
|---|---|
| Pub 100-17 Medicare Business Partners Systems Security | **Centers for Medicare & Medicaid Services (CMS)** |
| **Transmittal 12** | **Date: November 15, 2013** |
| | **Change Request 8460** |

**SUBJECT: CMS Business Partners Systems Security Manual**

**I. SUMMARY OF CHANGES:** The purpose of this update is to communicate changes to CMS and NIST requirements and procedures to Medicare Contractors.

**EFFECTIVE DATE: January 17, 2014**
**IMPLEMENTATION DATE: January 17, 2014**

***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** | 1/Introduction |
| **R** | 1.1/Additional Requirements for MACs |
| **R** | 2.1/CMS Contracting Officer's Representative (COR) |
| **R** | 2.2/Principal Systems Security Officer (SSO) |
| **R** | 3/IT Systems Security Program Management |
| **N** | 3.01/Control Components |
| **N** | 3.02/Reporting Requirements |
| **R** | 3.1/System Security Plan (SSP) |
| **R** | 3.2/Risk Assessment (RA) |
| **R** | 3.3/Contingency Planning |
| **R** | 3.4/Certification |
| **R** | 3.5.1/Annual FISMA Assessment (FA) |
| **R** | 3.5.2/Plan of Action and Milestones (POA&M) |
| **R** | 3.5.2.1/Background |
| **R** | 3.5.3/Timing Requirements for Compliance Conditions |
| **R** | 3.6/Security Incident Reporting and Response |
| **R** | 3.7/System Security Profile |

| R/N/D | CHAPTER / SECTION / SUBSECTION / TITLE |
|---|---|
| **R** | 3.8/Authorization To Operate |
| **R** | 3.10/Patch Management |
| **R** | 3.11.1/Security Configuration Management |
| **R** | 3.11.2/Security Technical Implementation Guides (STIG) |
| **R** | 3.11.3/United States Government Configuration Baseline (USGCB) Standard |
| **R** | 3.11.4/National Institute of Standards and Technology (NIST) |
| **R** | 4.1.2/Security Level by Information Type |
| **R** | 4.1.4/Minimum System Security Requirements - High |
| **R** | 4.3/Encryption Requirements for Data Leaving Data Centers |
| **R** | 5/Internet Security |

**III. FUNDING:**

**For Fiscal Intermediaries (FIs), Regional Home Health Intermediaries (RHHIs) and/or Carriers:**
No additional funding will be provided by CMS; contractor's activities are to be carried out within their operating budgets.

**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 obliged 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. 100-17 | Transmittal: 12 | Date: November 15, 2013 | Change Request: 8460 |
|---|---|---|---|

**SUBJECT: CMS Business Partners Systems Security Manual**

**EFFECTIVE DATE: January 17, 2014**
**IMPLEMENTATION DATE: January 17, 2014**

## I. GENERAL INFORMATION

**A. Background:** This is an update to the existing Business Partners Systems Security Manual (BPSSM). The BPSSM provides clarification and support to various CMS security policies, standards guidelines and procedures.

**B. Policy:** Compliance with the Federal Information Security Management Act of 2002, NIST requirements and guidance, and CMS policies, standards, guidelines and procedures.

## II. BUSINESS REQUIREMENTS TABLE

*"Shall" denotes a mandatory requirement, and "should" denotes an optional requirement.*

| Number | Requirement | Responsibility | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A/B MAC | | | DME MAC | FI | CARRIER | RHHI | Shared-System Maintainers | | | | Other |
| | | A | B | HHH | | | | | FISS | MCS | VMS | CWF | |
| 8460.1 | Contractors shall be in compliance with the requirements outlined in the updated Business Partners Systems Security Manual. | X | X | | X | | | X | X | X | X | X | |

## III. PROVIDER EDUCATION TABLE

| Number | Requirement | Responsibility | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | A/B MAC | | | DME MAC | FI | CARRIER | RHHI | Other |
| | | A | B | HHH | | | | | |
| | None | | | | | | | | |

## IV. SUPPORTING INFORMATION

**Section A: Recommendations and supporting information associated with listed requirements: N/A**

*"Should" denotes a recommendation.*

| X-Ref Requirement Number | Recommendations or other supporting information: |
|---|---|

**Section B: All other recommendations and supporting information: N/A**

## V. CONTACTS

**Pre-Implementation Contact(s):** Gregg Sanders, 410-786-1936 or Gregg.Sanders@cms.hhs.gov , Kevin Potter, 410-786-5686 or Kevin.Potter@cms.hhs.gov

**Post-Implementation Contact(s):** Contact your Contracting Officer's Representative (COR) or Contractor Manager, as applicable.

## VI. FUNDING

**Section A: For Fiscal Intermediaries (FIs), Regional Home Health Intermediaries (RHHIs), and/or Carriers:**
No additional funding will be provided by CMS; contractor's 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 do 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. 12, Issued:11-15-13)*

# CMS/ Business Partners
# Systems Security Manual

## Record of Changes

***(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)***

| Revision | Major Changes | Date |
|---|---|---|
| *12* | *Main Document and all Appendices*<br>*(1) Contract Officer Technical Representative (COTR) changed to Contracting Officer's Representative (COR) throughout document*<br>*(2) Updated Internet hyperlinks throughout document*<br>*(3) Changed "OCISO" (Office of the Chief Information Security Officer) to "EISG" (Enterprise Information Security Group) throughout document*<br>*(4) Changed C&A Program Procedures to SA&A Process throughout document*<br>*(5) Added Key Requirements throughout document*<br>*(6) Change IS to information security*<br>*(7) Change IS SSP to security plan*<br>*(8) Change RA to risk assessment*<br>*(9) Correct typographical errors*<br><br>*3.01: Created section. Moved policies and procedures paragraphs to section. Added Technical Implementation, Standards and Management Review paragraphs*<br><br>*3.02: Created section: Moved Reporting Requirements paragraphs and table 3.1 to section.*<br><br>*Table 3.1: Change SAS70 to Statements on Standards for Attestation Engagements (SSAE) 16*<br><br>*3.4: Certification* | *08/2013* |

*3.5.1: Removed CMS CO paragraph regarding the right to mandate which controls are tested. Added sentences regarding controls testing over 3 years*

*3.5.3: Added paragraph describing 6 month, monthly and weekly requirements*

*3.6: Added two background paragraphs, added TLS paragraph*

*Table 3.2: Removed old table and added updated table*

*Table 3.3: Deleted the table*

*3.9: Delete reference to rotation of duties*

*3.10: Added guidance statement and Table 3.3*

*3.11: Added Table 3.4*

*3.11.3: Replace section for FDCC with section for USGCB*

*4.1.4: Remove reference to PISP*

*4.3: Remove paragraphs regarding the CMS PISP and controls MP-5, MP-5(2) and MP-5(3), added language from CMS guidance*

*5: Update Technical Reference Architecture reference to version 3, added NIST Special Publications*

# CMS/Business Partners
# Systems Security Manual

## Table of Contents

***(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)***

### Table of Contents

# Appendices

Appendix A Medicare Information Technology (IT) Systems Contingency Planning

Appendix B An Approach to Fraud Control

# 1 - Introduction

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*This manual addresses the following key business partner security elements:*

- *An overview of primary roles and responsibilities*
- *A program management planning table to assist System Security Officers (SSOs) and other security staff in coordinating system security programs at business partner sites*
- *The collection of CMS policies, procedures, standards, and guidelines can be found on the CMS Information Security Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html*

The Centers for Medicare & Medicaid Services (CMS) requires that its business partners implement information security controls on their information technology (IT) systems to maintain the confidentiality, integrity, and availability (CIA) 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 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 Part A/Part B Medicare Administrative Contractors [ABMAC]).

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) - *Section* 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 MACs 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 MACs.

## *1.1 - Additional Requirements for MACs*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

MACs are responsible for fulfilling all existing business partner requirements. Additional requirements are specified in Section 912 of the 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 Security *Assessment and Authorization (SA&A) Process*, policies, standards, and guidelines for contractor facilities and systems. *Information on the* CMS *SA&A process* can be found on the CMS Web site at: *http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html*

- The contractor shall conduct or undergo an independent security control assessment 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 contract.

- The contractor shall support CMS validation and authorization of contractor systems and facilities in accordance with the CMS *SA&A Process*.

- The contractor shall provide annual certification, in accordance with the CMS *SA&A Process*, 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 *information security* requirements. The contractor's principal 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

## *2.1 - CMS Contracting Officer's Representative (COR)*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

CMS *CORs* oversee the business partners and also have Federal Acquisition Regulation (FAR) responsibilities at data centers. The *COR* has the following responsibilities:

- CMS point of contact for business partner *information security* problems
- Provider of technical assistance necessary to respond to CMS *information security* policies and procedures

## *2.2 - Principal Systems Security Officer (SSO)*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*Business partners shall designate a principal (i.e., primary) SSO qualified to manage the Medicare information 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.*

*See Section 1.1 for additional requirements that pertain to the Medicare Administrative Contractor SSO position.*

The principal 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 senior 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 the CMS information security program and CMS Minimum Security Requirements (CMSRs) by:

- Facilitating the Medicare IT system information security program and ensuring that necessary safeguards are in place and working
- Coordinating information security system activities throughout the organization
- Ensuring that IT system information security requirements are considered during budget development and execution
- Reviewing compliance of all components with the CMSRs 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 information 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 information security requirements are included in Requests for Proposal (RFP) and subcontracts involving the handling, processing, and/or analysis of Medicare data
- Maintaining information security documentation in the System Security Profile for review by CMS and external auditors and keeping all elements of the System Security Profile (see section 3.7)
- Cooperating in all official external evaluations of the business partner's information 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 3.3)
- 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/or following the issuance of new requirements, risk assessments, internal audits, and external evaluations.
- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix A)

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 conducted at the *CMS Security Controls Oversight and Update Training (CSCOUT)* can be used toward fulfilling the continuing professional education credits. The qualifying sessions and associated credit hours will be noted on the *CSCOUT* agenda.

# 3 - IT Systems Security Program Management

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*The Security Program consists of several fundamental components that are all designed to implement controls and to reduce risk. Key elements of controls include Policies, Procedures, Technical Implementations, Standards, and Management Reviews. Required documentation includes, but is not limited to, the security plan, the risk assessment, and the contingency plan.*

Business partners shall *implement an IT Systems Security Program to manage the system security risks. Risks are identified by the business partner in the Information Systems Risk Assessment (see section 3.2) and the security requirements are documented in the System Security Plan (see section 3.1). The underlying support for these documents is the controls implemented by the business partner.* Controls are measures implemented to protect the CIA of sensitive information. Information security controls shall be implemented in a consistent manner everywhere within the system's accreditation boundary. 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 information security controls are operating as intended.

## *3.01 - Control Components*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

*Business partners shall have policies and procedures, and implement controls or plans that fulfill the CMSRs (see CMS Information Security Acceptable Risk Safeguards (ARS) including CMS Minimum Security Requirements). The business partner Medicare claims related security program shall be based on the collection of CMS policies, procedures, standards, and guidelines found on the CMS Information Security Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html.*

***Policies** are formal, up-to-date, documented rules that are tailored to the environment, are communicated as "shall" or "will" statements 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.*

***Technical Implementations** are the acquisition and installation of hardware, software, or assets to be used for the establishment of a new control, or the improvement of an existing control. The intention of a technical implementation is to automate or facilitate a control process that would otherwise be manually performed.*

***Standards** are formal, written, mandatory actions, rules, or specifications designed to support and conform to a policy or procedure. A standard must include one or more accepted specifications for configurable items for hardware, software, or behavior. Standards are often required to successfully complete technical implementations and can be either part of policies and procedures, or can be standalone documents. Standards can result from, either exclusively by or in combination with, laws promulgated by governing bodies, obtained from known standards organization or developed by the business partner using industry best practices.*

***Management Review** is the business partners' formal oversight activity of the control implementation and should be performed at various management levels. Oversight is a regular activity to verify that the control environment for which management has responsibility is functioning properly. Management must set benchmarks or other methods to measure the success of controls. Where appropriate, management should document their review by formally approving evidence supplied.*

## *3.02 - Reporting Requirements*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*Business partners are required to provide documentation to CMS regarding the status of their IT security program. Documentation shall be reported to CMS according to the appropriate procedures, which are summarized in Table 3.1.*

*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 their high-level descriptions. 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 Federal Information Security Management Act of 2002, 44 U.S.C. §3541 (FISMA) Assessment (FA) using the CMS FISMA Controls Tracking System (CFACTS). The weaknesses, action plans, and POA&Ms shall be recorded in the CFACTS (See Risk Management Handbook [RMH] Volume II Procedure 6.2 POA&M Management). To perform the FA, business partners shall conduct a systematic review of the CMSRs using the CFACTS. CFACTS provides a "Control Response" form that includes guidance and assessment procedures to assist in the review of the CMSRs.*

*In addition, 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 that 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.*

*Table 3.1. Reporting Requirements Planning Table*

| *Requirement* | *Frequency* | *Send To* | *Comments* | *Complete (check when complete)* |
|---|---|---|---|---|
| *CMS POA&M & Annual FISMA Assessment* | *One third of the controls shall be tested each year so all controls are tested during a 3-year period.* | • *COR with a copy to CMS CO via CFACTS*<br>• *System Security Profile* | *See RMH Volume II Procedure 4.2 for an overview of the FA.*<br><br>*FA results recorded in the CFACTS are to be discussed in the Certification Package for Internal Controls (CPIC) Certification Package.* | |
| *3.1 Security Plan* | *The security plan for each General Support System (GSS) and MA shall be reviewed, updated, and certified by management every 365 days, or upon significant change[1].* | • *SSO*<br>• *CMS CO via CFACTS*<br>• *System Security Profile* | *Information system security plans are to be reviewed, updated, and certified by management and indicated as such in both the CFACTS, the CPIC Certification Package/Statement of Certification, and the System Security Profile[2].* | |

*[1] 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) |
|---|---|---|---|---|
| *3.2 Risk Assessment* | *The risk assessment for each GSS and MA shall be reviewed, updated, and certified by management every 365 days, or upon significant change.[1]* | • *CMS CO via CFACTS*<br>• *System Security Profile* | *Risk assessments are to be reviewed, updated, and certified by management and indicated as such in the CFACTS, the CPIC Certification Package/Statement of Certification, and the System Security Profile. The risk assessment is submitted with the security plan[3].* | |
| *3.3 Certification* | *Each federal FY* | • *COR with a copy to CMS CO via CFACTS*<br>• *System Security Profile* | *FIs 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 shall be submitted. All other contractors should submit a statement of security certification to their CMS CORs.* | |
| *3.4 Contingency Planning* | *CPs shall be reviewed, updated, and certified by management every 365 days, or upon significant change.[1]*<br><br>*CPs shall be tested annually.* | • *SSO*<br>• *CMS CO via CFACTS*<br>• *System Security Profile* | *Management and the SSO shall approve the CP.*<br><br>*The CP is to be developed (in accordance with Appendix A and CMS CP procedures), reviewed, updated, and certified by management—and indicated as such in the CFACTS, the Certification Package/Statement of Certification, and the System Security Profile[4].* | |
| *3.5 Compliance* | *Each federal FY* | • *SSO*<br>• *COR*<br>• *CMS CO via CFACTS*<br>• *System Security Profile* | *POA&M: POA&Ms address findings of internal/external audits/reviews including annual security assessments, and, as applicable: Statements on Standards for Attestation Engagements (SSAE) 16 reviews, Chief Financial Officer (CFO) controls audits, the Section 912 evaluation, and data center tests and reviews.* | |

*[2] More information about system security planning can be found in the CMS Information Security (IS) System Security Plan (SSP) Procedures.*
*[3] More information about Risk Assessment Reports can be found in the CMS risk assessment procedures.*
*[4] More information about contingency planning can be found in NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, and NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.*

| Requirement | Frequency | Send To | Comments | Complete (check when complete) |
|---|---|---|---|---|
| *3.6 Incident Reporting and Response* | *As necessary* | • *COR*<br>• *CMS IT Service desk*<br>• *Medicare Contractor Management Group (MCMG) Security Mailbox (See the latestest guidance from CMS for more information)*<br>• *System Security Profile* | *Health Insurance Portability and Accountability Act (HIPAA) also addresses Incident Reporting information.* | |
| *3.7 System Security Profile* | *As necessary* | *On file with the Principal SSO* | | |
| *3.8 Authorization To Operate* | *As necessary to acquire and maintain a CMS CIO-granted Authorization to Operate.* | *On file with CMS Enterprise Information Security Group (EISG), with a copy maintained in the CFACTS.* | | |

*LEGEND:*

| | |
|---|---|
| *CFACTS* | *CMS FISMA Controls Tracking System* |
| *CFO* | *Chief Financial Officer* |
| *CO* | *Central Office (CMS)* |
| *COR* | *Contract Officer Representative* |
| *CP* | *Contingency Plan* |
| *CPIC* | *Certification Package for Internal Controls* |
| *FA* | *FISMA Assessment* |
| *FY* | *Fiscal Year* |
| *GSS* | *General Support System* |
| *HIPAA* | *Health Insurance Portability and Accountability Act* |
| *IT* | *Information Technology* |
| *MA* | *Major Application* |
| *POA&M* | *Plan of Action and Milestones* |
| *RA* | *Risk Assessment* |
| *SSAE* | *Statement on Standards for Attestation Engagements* |
| *SP* | *Special Publication (NIST)* |
| *SSO* | *Business Partner Systems Security Officer* |

*NOTE: The documents listed in Table 3.1 may be stored as paper documents, electronic documents, or any combination thereof.*

*When submitting documentation to the CMS CO, Registered Mail™ or its equivalent (signed receipt required) shall be used. For supporting documentation (such as RAs, CPs, security plans, etc.), only electronic copies in the approved CMS format are required. Paper copies are only required for certification signature pages, certifying the completion of required periodic document development, review, updates, and certification. Contact addresses are as follows:*

*Program Safeguard Contractors (PSC) and Zone Program Integrity Contractors (ZPIC)*

- *CMS Central Office*

*Center for Program Integrity*
*Division of Benefit Integrity Management Operations*
*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*
  *Center for Medicare*
  *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. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*Business partners are required to update and re-certify the SSP every 365 days unless there are changes that would necessitate a more frequent update. Updates to the SSP shall be performed in accordance with procedures available on the CMS Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html.*

*Defining a system boundary is a key step that must be completed before a SSP can be accurately documented.*

*The SSP should address how the control environment is implemented to mitigate risks identified in the risk assessment.*

The objective of an *information security* program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process, transmit, or store Medicare-related data have some level of sensitivity and require protection. The protection of a system shall be documented in a *security plan*. The completion of an *security plan* is a requirement of the Federal Information Security Management Act of 2002 (FISMA), Privacy Act of 1974, As Amended, *Office of Management and Budget (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 an MA or GSS shall be covered by *security plans*.

The purpose of a *security plan* is to provide an overview of the security requirements of a system and describe the controls that are implemented to meet those requirements. The *security plan* also delineates responsibilities and expected behavior of all individuals who access the system. The *security plan* 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 Business Owners, information owners, the system operator, and the system security manager (i.e., SSO).

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

The *security plans* shall be available to the SSO and business partner certifying official (normally the Vice President [VP] for Medicare Operations), and authorized external auditors as required. The SSO and Business Owner are responsible for reviewing the *security plan* 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 *security plans* shall be developed in accordance with the most current version of the CMS *security plan* procedures available on the CMS Web site at: *http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html*.

*Security plans* shall be re-certified within 365 days from the previous certification date. The *security plan* shall also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update is required. The *security plan* 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 or the updated *security plan*, if applicable, shall be *recorded in the CFACTS*, placed in the System Security Profile, and a copy shall be submitted to the CMS CO.

Contractors updating their current *security plan*(s) or developing new *security plan*(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 *security plan* procedures.

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 forms, post-payment medical reviews, customer service, appeals, overpayment written/phone inquiries and separate claims reconciliation systems.

A newly developed or updated *security plan* shall be maintained in the CFACTS and sent in electronic form to the CMS CO on CD-ROM. This CD-ROM must be received by CMS 10 working days after the *security plan*(s) has been developed, updated, or re-

certified. The original signed, dated CMS *security plan* certification form shall be submitted in paper copy form along with the CD-ROM electronic copy. This information shall not be submitted to the CMS CO via e-mail—Registered Mail™ or its equivalent (signed receipt required) shall be used.

## *3.2 - Risk Assessment (RA)*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***

*Business partners are required to perform an annual risk assessment in accordance with the most current versions of the CMS risk assessment procedures available on the CMS Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html. The identified risks will aid in the design of controls to satisfy the CMSRs.*

*Documentation of the risks needs to be completed before a control is designed and implemented. Controls should be designed to be cost effective based on the risk.*

*Risks never go away, but their ratings can increase as new vulnerabilities are found and decrease as new or enhanced controls are implemented.*

The CMS *risk assessment* procedures present a systematic approach for the RA process of Medicare information computer systems within the CMS and business partner environments. The procedure describes the steps required to produce an *risk assessment* for systems and applications.

All business 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 *risk assessment* procedures shall be used to prepare an annual *risk assessment*.

*Risk assessments* shall be re-certified within 365 days from the previous certification date. The *risk assessment* shall also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update is required. The *risk assessment* 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 or the updated *risk assessment*, if applicable, shall be placed in the System Security Profile, and a copy shall be submitted to the CMS CO. Note that the *risk*

*assessment* used to support a *security plan* cannot be dated more than 12 months earlier than the *security plan* certification date.

Contractors that must update their current *risk assessment*(s) shall use the most current versions of the CMS *risk assessment* procedures.

A newly developed or updated *risk assessment* that is submitted with the *security plan* shall be maintained in the CFACTS and sent to the CMS CO on CD-ROM. The CD-ROM must be received by CMS 10 working days after they have been developed and/or updated. This information shall not be submitted to the CMS CO *via e-mail*—Registered Mail™ or its equivalent (signed receipt required) shall be used.

In summary, the *risk assessment* shall be updated annually unless there are changes (as discussed above) that would necessitate a more frequent update. Should *risk assessment* technical assistance be required, direct all questions to the CMS *Enterprise* Information Security *Group (EISG)* at mailto:CISO@cms.hhs.gov.

## *3.3 - Contingency Planning*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*Business partners are required to document and test an IT Systems Contingency Plan in accordance with the most current versions of the CMS Information Security Contingency Planning procedures available on the CMS Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html.*

All business partners are required to develop and document a Contingency Plan (CP) that describes the arrangements that have been implemented and the steps that shall be taken to continue IT and system operations in the event of a natural or human-caused disaster. 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, *DME*]), each individual Medicare contract type shall be tested every year.

Appendix A to this manual provides information on Medicare IT systems contingency planning and testing methods. See *requirement* 3.4 in Table 3.1, *which is contained in* section 3.*02*, for other references.

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

A newly developed and/or updated IT Systems CP shall be updated in CFACTS and submitted to CMS within 10 working days after the business partner's management and SSO have approved it. A copy of the IT Systems CP shall be submitted via CD-ROM to the CMS CO along with a paper copy of the statement of certification. This information shall not be submitted via e-mail—Registered Mail™ or its equivalent (signed receipt required) shall be used.

## 3.4 - *Certification*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

All business partners are required to certify their system security compliance. Certification is the formal process by which a contractor official verifies, initially and then by annual reassessments, that a system's security features meet the CMSRs. Business partners shall self-certify that their organization successfully completed an annual, independent FA 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 information security compliance within each federal FY. This security certification shall be included in the CPIC package or, for contracts not required to submit CPICs, send the security certification to their appropriate CMS CORs. CMS shall continue to require annual, formal re-certifications within each FY 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 the System Security Profile. 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 Annual Security Control Assessment
- System Security Plan for each GSS and MA (see section 3.1)
- Risk Assessment (see section 3.2)

- IT Systems Contingency Plan (see section 3.3 and Appendix A)

- Plan of Action and Milestones (see section 3.5.2)

### *3.5.1 - Annual FISMA Assessment (FA)*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*At least 1/3 of controls must be testing each year, and all controls shall be tested over a 3 year period.*

*CMS reserves the right to identify which control families must be tested each year.*

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 annual FA is documented, tracked, and reported in the CFACTS. The purpose of annual FA 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 FA is intended to validate the CMSRs to determine the extent to which the controls are:

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

The annual FA testing requirement has been interpreted by OMB as being within 365 calendar days of the prior test. Over a 3-year period, all CMSRs applicable to a system or application shall be tested. This means a subset (no less than one-third [$^1/_3$]) of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period. *In an effort to standardize testing and results summarization, a 3-year rotation of CMSR control families was established by CMS. As control families are added or removed, CMS CO reserves the right to change the controls that must be tested each year.*

To fulfill the annual FA validation obligation, the FA shall be conducted by an independent agent or team. This can be any internal/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 CMSR effectiveness. All management-directed and independent testing conducted with*in* 365 days of the attestation due date may be used to meet the requirement for the annual security controls (i.e., FA) testing.

## *3.5.2 - Plan of Action and Milestones (POA&M)*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*Business partners are required to prepare a monthly POA&M update which is due by the 1st of each month. The POA&M update consists of updating all active POA&M items in the CFACTS and, if required by CMS, uploading any additional supporting documentation.*

### *3.5.2.1 - Background*

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 any covered system 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 MACs and existing carrier and FI 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 (i.e., weaknesses) 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 CFACTS enables contractors to satisfy reporting requirements for EDP security-related findings. Security-related findings and approved action plan data is promptly entered into the CFACTS following all audits/reviews, from which the CFACTS provides a single monthly submission report that summarizes the current state of security for the business partner.

### *3.5.3 - Timing Requirements for Compliance Conditions*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

Many security documents, such as *risk assessments, security plans*, Contingency Plans, as well as many CMSR control requirements (see CMS Information Security Acceptable Risk Safeguards [ARS], CMS Minimum Security Requirements Appendices A, B, and C) 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 FA submission.

If the business partner wishes to change the timing cycle of an annual or yearly requirement compliance date, the business partner is required to 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 *security plan* is 7/31/*13* and the business partner desired to change the review date to 5/31/*14*, they would be required to review the *security plan* no later than 7/31/*13*, again no later than 5/31/*14*, and no later than 5/31/yy thereafter.

*For other controls, there may be a requirement they be performed every 6 months, monthly or weekly. To express this in terms of days, every 6 months shall be completed within the range of 181 - 184 days. Monthly controls shall be performed within the range of 28 - 31 days and weekly controls shall be performed within 7 days. The only exception to this is if a monthly or weekly control falls on a non-business day, the control can be completed on the next business day, but the next control process must return to the normal cycle. For example, if a weekly control is normally performed on a Friday, but one Friday is a holiday, the control can be performed on the next business day (i.e., Monday). The control must then be performed again on the upcoming Friday, which would be 4 days later.*

### *3.6 - Security Incident Reporting and Response*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*All security incidents shall be reported to CMS in accordance with the requirements listed in Table 3.2. Incidents shall be reported to the IT Service Desk.*

A security 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. Upon receiving notification of an IT systems security incident or a suspected incident, the SSO or another identified individual 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.

All suspected *security incidents* or events shall be reported to the business partner*'s* IT service desk (or equivalent business partner function) as soon as an incident comes to the attention of an information system user. All security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS *RMH Volume II Procedure 7.2* Incident Handling Procedures. This document is available on the CMS Web site at *http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html.* The CMS IT Service Desk can be contacted by telephone at *800-562-1963 or* 410-786-2580, or by e-mail at: mailto:CMS_IT_Service_Desk@cms.hhs.gov.

All CMS contractors and business partners shall *use* the incident categories and reporting time criteria, *contained in* Table 3.*2*, when reporting incidents to CMS.

Table 3.2. Incident Categories

| *Category* | *Name* | *Description* | *HHS Reporting Timeframe* |
|---|---|---|---|
| *CAT 0* | *Exercise /Network Defense Testing* | *This category is used during State, federal, national, and international exercises, and approved activity testing of internal/external network defenses or responses.* | *Not Applicable; this category is for each agency's internal use during exercises.* |
| *CAT 1* | *Unauthorized Access** | *An individual gains logical or physical access, without permission, to a federal agency network, system, application, data, or other technical resource.* | *Within one (1) hour of discovery/detection.* |
| *CAT 2* | *Denial of Service** | *An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources; this activity includes being the victim of or participating in the attack.* | *Within two (2) hours of discovery/detection if the successful attack is ongoing and the HHS Operating Division (OPDIV) is unable to successfully mitigate activity.* |

| Category | Name | Description | HHS Reporting Timeframe |
|---|---|---|---|
| CAT 3 | Malicious Code* | A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus software. | Within one (1) hour of discovery/detection if widespread across the agency/OPDIV. The total count of all CAT 3 incidents and events, (including those successfully quarantined), should be rolled up and reported monthly. |
| CAT 4 | Inappropriate Usage* | An individual violates acceptable use of any network or computer use policy. | Weekly |
| CAT 5 | Scans/Probes/ Attempted Access | 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 DoS. | Monthly (fifth day of the month for the previous month's data). |
| CAT 6 | Investigation | Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. | Weekly |

| *Category* | *Name* | *Description* | *HHS Reporting Timeframe* |
|---|---|---|---|
| *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.*<br><br>*Any incident that involves compromised PII must be reported within 1 hour of detection regardless of the incident category reporting timeframe.* | *Any incident that involves compromised PII must be reported within 1 hour of detection regardless of the incident category reporting timeframe* |

*Source: NIST SP 800-61 Rev. 1

When reporting confirmed security incidents, business partners shall report the date and time when events occurred or were first 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 Inspector General (*OIG*)* Computer Crime Unit and submit a report to the Federal Computer Incident Response Capability (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 shall 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 shall refer to The CMS Information Security Incident Handling and Breach Analysis/Notification Procedure for further guidance.

*Many of the PII breaches being reported to CMS occur when unencrypted emails are sent to the intended recipients. A mitigating control to allow many of these breaches to be closed more easily is the implementation of the Transport Layer Security (TLS) protocol*

*within email servers such as Microsoft Exchange. The TLS protocol encrypts emails for transmission between two email servers. There are different TLS features which can be used and provide different levels of assurance that an email will be encrypted. Use of any of these features requires TLS to be enabled. To mitigate the severity of email PII breaches, business partners are required to enable TLS on their email servers. In addition, the most secure TLS feature that can be enabled to encrypt emails between business partners shall be implemented. If a business partner cannot implement TLS, a risk must be documented in the RA.*

## *3.7 - System Security Profile*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*The System Security Profile is a copy of the documents that are maintained in CFACTS and on CMS Web sites. These documents would be available should business partner management require timely access to them without CFACTS or CMS Web site availability.*

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

- Completed FAs
- Security Plans (for each GSS and MA)
- Risk Assessments
- Certifications
- Contingency Plans
- POA&Ms for each compliance security review
- POA&Ms for other security review undertaken by *Department of Health and Human Services (HHS)* OIG, CMS, Internal Revenue Service (IRS), GAO, consultants, subcontractors, and business partner security staff
- Incident reporting and responses
- Systems *information 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.

## *3.8 - Authorization To Operate*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

Business partners are required to acquire and maintain a CMS CIO-issued Authorization to Operate (ATO) for each GSS and MA. The guide for Authorization To Operate is defined in the CMS Authorization To Operate Package Guide document, located at: *http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html*.

## *3.10 - Patch Management*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*The timely patching of systems is one of the critical controls to preventing network intrusions.*

*The CMSRs contain the time frames required to be met for timely patching. The time frame begins when the vendor releases a patch, not when the business partner becomes aware of a patch.*

Timely patching is critical to maintaining the operational CIA of Medicare systems. However, failure to keep operating system and application software patched is the most common mistake made by IT professionals. New patches are released daily and it is often difficult for even experienced system administrators to keep abreast of all the new patches. The Computer Emergency Response Team (CERT)/Coordination Center (CC) (http://www.cert.org) estimates that 95 percent of all network intrusions could be avoided by keeping systems up-to-date with appropriate patches.

To help address this growing problem, CMS recommends that business partners have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. The CMSRs provide specific guidance on time frames for implementing patches. *Further guidance is provided in Table 3.3 below for 1) Patch Identification, 2) Patch Installation and 3) Unsupported software.*

*Table 3.3*

| | |
|---|---|
| *Patch Identification* | *Include all patches that are released from the system, application, or device vendor.*<br><br>*All patches must be analyzed by the business partner to determine their applicability and security impact on the* |

| | |
|---|---|
| | *operating environment. All patches analyzed from the vendor must be tracked through a formal process and categorized as 1) Security or 2) Operational in nature.* |
| *Patch Installation* | *The CMSRs provide specific guidance on time frames for implementing patches.*<br><br>*Security related patches not installed based on business partner analysis shall be documented with an appropriate business justification.* |
| *Unsupported Software* | *Unsupported software, or software that is not formally supported by the software vendor for security or operational patches, shall not be used unless advanced patch support is purchased or provided through another documented source. All unsupported software in operation shall be documented within the Business Partner's IS RA and POA&M with phase out timelines defined.* |

NIST SP 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program, provides a valuable and definitive process for setting up, maintaining, and documenting a viable patch management process. CMS highly encourages business partners to utilize NIST and other guidance documents to develop configuration standards, templates, and management processes that securely configure Medicare systems as part of their configuration management program.

## *3.11.1 - Security Configuration Management*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

***Key Requirements***
*Business partners are required to create a security baseline configuration for the information system components.*

*Federal guidelines should be used to create baselines. If a Federal guideline does not exist, hardening guides or documented best practices may be used.*

*DMEMACs, ABMACs, and EDCs are responsible for starting their security configurations with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) Checklists.*

FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. CMS highly encourages business partners to utilize guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

Security configuration guidelines may be developed by different federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or CMS guideline. To resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing *Federal* security configuration guidelines follows. If there is a conflict between an ARS and a DISA STIG, *the ARS takes precedence. See Table 3.4 for more information*. If there are any *other* questions or concerns about resolving conflicts among security configuration guidelines, business partner SSOs shall contact their CMS Business Owner.

*Table 3.4*

| *Business Partners* | *DMEMAC/ABMAC/EDCs* |
|---|---|
| 1. *CMS ARS*<br>2. *USGCB*<br>3. *NIST National Checklist Program (NCP) / NIST*<br>4. *DISA* | 1. *CMS ARS*<br>2. *DISA/USGCB*<br>3. *NIST National Checklist Program (NCP) / NIST* |

## *3.11.2 - Security Technical Implementation Guides (STIG)*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

Security guidelines, called STIGs, and security configuration checklists, called Checklists, are available for most major operating systems, support applications, and infrastructure services. STIGs contain detailed guidance, best practices, and recommendations for configuring a particular product. Checklists are a tool that provides detailed instructions for checking the presence of a vulnerability identified in a STIG and configuring detailed system/application configuration settings. Both are developed by DISA to help system operators configure security within their systems to the highest level possible. All STIGs and Checklists are available from DISA. The link for STIGs and checklists is http://iase.disa.mil/stigs/checklist/index.html. CMS recommends that business partner SSOs (or their designated representative) subscribe to the DISA STIG-News Mailing List at: http://iase.disa.mil/help/mailing-list.html so they will be notified whenever updated or new STIG Checklists become available.

The use of latest publically available DISA STIG Checklists is mandatory for all business partner systems/applications that process, store, and/or transmit Medicare claims data. DMEMACs, ABMACs, and EDCs are required to start with the STIG baseline

configurations and then document any exceptions and/or deviations based on environment specific implementation. While it may not be possible to implement all of a STIG's recommended security settings because doing so would compromise the functionality of an application and/or system, CMS expects every business partner to analyze the STIG recommended settings and determine which ones are feasible, and to implement all settings that are found to be feasible. Settings that cannot be implemented on specific systems shall be documented as "system exceptions," and settings that cannot be implemented across an entire platform (e.g. Windows 200*8*, AIX) shall be documented as "system deviations." All STIG recommended security settings that are determined not to be feasible in a business partner environment shall be documented in the applicable system/application Security Configuration Checklist (SCC) with appropriate business justification (security impact, operational impact, business impact), mitigating or compensating controls, and residual risk.

### *3.11.3 - United States Government Configuration Baseline (USGCB) Standard*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

*The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration (FDCC) mandate. While not addressed specifically as the FDCC, the process (now termed the USGCB process) for creating, vetting, and providing baseline configurations settings was originally described in a 22 March 2007 memorandum from OMB to all Federal agencies and department heads and a corresponding memorandum from OMB to all Federal agency and department Chief Information Officers (CIO).*

*Business Partners have the choice of using the USGCB configurations or the STIGs for the platforms listed on the USGCB Web site at http://usgcb.nist.gov/index.html.*

### *3.11.4 - National Institute of Standards and Technology (NIST)*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) tasks 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, 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 (FIPS) Publications, 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 agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, any reference to a "waiver process" included in FIPS publications is no longer valid. 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 this *Business Partners Systems Security Manual (*BPSSM*)* and the *ARS*. 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.

The most current NIST publications are available at:
http://csrc.nist.gov/publications/index.html.

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 - Information And Information Systems Security

## *4.1.2 - Security Level by Information Type*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

Using FIPS 199, 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 many information types processed on and/or by CMS information systems. These information types are defined in the *Risk Management Handbooks RMH*

*Vol II Procedure 2-3 Categorizing an Information System and RMH Vol III Standard 3-1 Authentication (for e-authentication), located at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html*. For each information type, CMS used FIPS 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., CMSRs).

### *4.1.4 - Minimum System Security Requirements—HIGH*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

FIPS 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 200, agencies shall first determine the security category (i.e., information type) of their information system in accordance with the provisions of FIPS 199, and then apply the appropriate set of baseline security controls contained in NIST SP 800-53 *Rev. 3* (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 *Rev. 3*. 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 *and Privacy* Program individual policy statements, along with the CMS Minimum Security Requirements Procedure 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' information and information systems. These two CMS documents, along with other federal and CMS requirements, form the basis for the CMSRs.

### *4.3 - Encryption Requirements for Data Leaving Data Centers*

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

CMS, as a trusted custodian of individual health care data, must protect its most valuable assets—its information and its information systems. Consequently, CMS believes that putting the government's credibility at risk is not acceptable.

Effective immediately, and until further notice, no data that includes personally identifiable information (PII) shall be transported from a CMS data center (including business partner data centers and subcontractor data centers) unless it has been encrypted.

*The only exception to this requirement is for hardcopy records that are transported to and from an off-site location and between off-site locations. To qualify for this exception, the controls listed below (additional information is available from CMS) shall be used.*

*To prepare the records for shipment:*

- *The records shall be stored in boxes.*
- *Each box shall be uniquely identified.*
- *Boxes shall be secured for shipment.*
- *Secured boxes shall be loaded into the shipping container or vehicle.*
- *Total items in each shipment shall be noted and the Bill of Lading signed.*
- *At time of pickup, the shipping company representative shall verify and sign the Bill of Lading.*
- *A copy of the identification records shall accompany each shipment.*
- *The shipping container or vehicle shall be locked and sealed with the seal number noted on the Bill of Lading.*
- *A copy of the completed Bill of Lading shall be kept by the contractor.*

*Upon receipt of the shipment at the storage facility:*

- *A storage facility representative shall verify the seal number and that it is unbroken.*
- *Compare the contents of the shipment against the Bill of Lading and the boxes against the copy of the identification record.*
- *If any discrepancies are found, the discrepancy shall be immediately resolved.*
- *After verification that all boxes shipped were received, information from the Bill of Lading shall be sent to the shipper where it shall be verified.*
- *Within 24 hours, all boxes on each shipment shall be scanned into the storage facility's tracking system and inserted into the storage racks.*

# 5 - Internet Security

*(Rev. 12, Issued: 11-15-13, Effective: 01-17-14, Implementation: 01- 17-14)*

With prior written approval of their sponsoring CMS Business Owner, business partners may now use Internet technology for transmission of and/or receipt of health care transactions. Each request for using Internet technology will be considered individually and approval is not automatic. However, any approval shall require that business partners meet CMS architectural, security, data interchange, and privacy requirements for Internet-facing infrastructure. Further, an independent (third-party) *Security Control Assessment* of the new functionality prior to its release into production is required and the *Security Control Assessment* must include penetration testing. The *Security Control Assessment* is conducted to validate compliance with the following specific architectural, security, data interchange, and privacy requirements, as well as the CMSRs. The *Security*

*Control Assessment* must be conducted by a CMS-contracted third party. The existing requirement for an annual penetration test of the contractor network shall include any approved Internet infrastructure. Compliance with existing requirements to conduct quarterly vulnerability scans and annual penetration testing is still mandatory.

Briefly, architectural, security, data interchange and privacy requirements include the following:

1. Architecture:

    - Explicit compliance with CMS system lifecycle standards, particularly:
        - CMS Technical Reference Architecture, Version *3*.0, and all its appendices, and
        - CMS Java EE Application Development Guidelines.
    - Utilization of resources to leverage existing technology and solutions such as platform and software developed by contractors and in compliance with CMS standards to meet the same or similar business requirements. The technology and solutions would also have to align with requirements for the Medicare Administrative Contractors, Enterprise Data Centers, and Standard Front End initiatives.

2. Security:

    - Full compliance with the CMS Integrated IT Investment & System Life Cycle Framework (Checkpoints, Deliverables, and Activities including *Security Authorization*) in introducing the new functionality.
    - Satisfactory systems test and evaluation of the Internet application to include evaluation of all control categories set forth in the CMSRs.
    - Compliance with DHHS and CMS standard configuration settings.
    - Compliance with the NIST SP 800-41 *Rev. 1*, Guidelines on Firewalls and Firewall Policy; NIST SP 800-44 *Version 2*, Guidelines on Securing Public Web Servers; *NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) NIST 800-111, Guide to Storage Encryption Technologies for End User Devices; NIST SP 800-113, Guide to SSL VPNs; NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access;* NIST SP 800-115, Technical Guide to Information Security Testing and Assessment; NIST SP 800-119, Guidelines for the Secure Development of IPv6; and NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing.
    - *Security Authorization* dependent on compliance with security control requirements and completion of documentation such as the *risk assessment*, the *security plan* for the infrastructure, platform, and applications supporting the Internet functionality, and a CP for the supporting platform and application. The risk assessment must address e-authentication requirements and controls for electronic transactions, or refer to a separate document if one exists. All security documentation must be developed to the CMS methodologies and procedures

provided at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

3. Privacy: Completion of a Privacy Impact Assessment (PIA) as set forth in Section 208 of the E-Government Act.

4. Data Interchange:

   - Utilization of HIPAA compliance standards for applicable transactions (i.e. claims, remittances and inquiry/response for eligibility and claim status) to be enabled by the new functionality.
   - Enabling both batch file transfer and interactive screen presentation for the HIPAA transactions.
   - 508 compliance for interactive screen presentation.
   - All Internet and non-Internet data exchange modes (i.e. Interactive Voice Recognition, Direct Data Entry, and Computer to Computer) shall return consistent data.
   - Compliance with Trading Partner authentication requirements including submitter/provider relationship for the HIPAA transactions.

Application requirements include but are not limited to the following:

1. A proof of concept/concept of operation paper describing the new application and functionality.
2. Information that the Internet service shall be extended only to entities or providers enrolled in the jurisdiction of the proposing business partner.
3. An attestation that the applicant has had a similar private-side application that has been in production for more than one year. The attestation shall describe the experience of the private-side application and how it relates to the Internet proposal.

Other application requirements may be imposed by the sponsoring CMS business component.

Additionally, business partners may also use the Internet for: 1) utilizing the IRS Filing Information Returns Electronically (FIRE) system for Form 1099 submissions, and 2) utilizing e-mail to transmit sensitive information via encrypted attachments in accordance with all applicable CMSRs. An application for these uses is not required. If not already emplaced, contractors must install firewalls, filtering technology to screen incoming e-mail for high risk transmissions such as executables, up-to-date virus protection software, and intrusion detection software to utilize the Internet for these purposes.