Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS INFORMATION SECURITY (IS) PLAN OF ACTION & MILESTONES (POA&M) PROCEDURE

June 15, 2009

Version1.1- Final

SUMMARY OF CHANGES IN CMS IS POA&M PROCEDURE V1.1

1. This document replaces the *CMS Information Security Plan of Action and Milestones (POA&M) Guidelines*, dated July 6, 2007.
2. Title Change – The title of the document is changed to the *CMS Information Security (IS) Plan of Action and Milestones (POA&M) Procedure*.
3. Summary of Changes – Added the Summary of Changes to provide an overview of the changes that were implemented in this version of the document.
4. Executive Summary – Added an Executive Summary to the document to provide a summary description of the contents and layout of the CMS IS POA&M Procedure.
5. Section 3.6 – Changed CAP reference from Section 7 to Section 6.
6. Attachment C – Internal Justification for Closure Instruction and Template, B-Notification Memo Template – Added additional completion instructions.
7. Attachment D – CMS IS Policy/Standard Risk Acceptance Template – Added template.
8. General Formatting – Changes were made throughout the document to support CMS IS standards.
9. General Formatting – Changes were made throughout the document to bring the document into compliance with Section 508.

EXECUTIVE SUMMARY

This document replaces the *Centers for Medicare and Medicaid Services (CMS) Information Security (IS) Program Plan of Action and Milestones (POA&M) Guidelines,* dated July 6, 2007. The *CMS Information Security Plan of Action and Milestone Procedure* provides CMS management and Business Owners with the necessary information and instructions for developing, maintaining and reporting their weaknesses in IS as it relates to a specific information system. The CMS IS POA&M Procedure complies with the requirements prescribed by the Office of Management and Budget (OMB). Information is included to account for the emphasis that has been placed on formalizing the weakness mitigation process and ensuring weaknesses are appropriately prioritized for mitigation.

A POA&M is a management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The CMS IS POA&M process will be used to facilitate the remediation of IS program- and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions;
- Defining roles and responsibilities for weakness resolution;
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses;
- Tracking and prioritizing resources; and
- Informing decision makers.

POA&Ms are used to assess the state of the CMS' IT Security and to aid in oversight of IT investments. OMB requires tying the POA&M to the budgeting process to evaluate the soundness of an investment. Systems that do not adequately address a plan for securing funding for mitigation of IT security weaknesses can be placed 'at risk' and lose funding. For major investments, OMB requires related POA&Ms to be cross-referenced through answers to questions when completing section II.B of an Exhibit 300. The response to all questions in this section of the Exhibit 300 should align with weaknesses reported in the POA&M that require funding.

The POA&M process provides significant benefits to both CMS and DHHS. It is a dynamic management tool useful for ongoing efforts to address programmatic and system-specific vulnerabilities. It assists in essential decision-making activities, facilitating and helping to ensure the oversight and mitigation of security weaknesses and the cost-effective use of mitigation resources. To function effectively, POA&Ms must be continually monitored and diligently updated. A mature POA&M process requires that the knowledge and efforts of each CMS component are sustainable over time, independent of any organizational and personnel changes. An effective POA&M captures each of these changes completely and concisely.

This document was designed to be alignment with the DHHS POA&M Guide. Section 1 provides the introduction, purpose, scope and a description on how to use the Procedure. Sections 2-5 and Section 7 of this document provide the CMS implementation of the DHHS guidance. Section 6 provides the instructions of how to manually submit the Corrective Action

Plans (CAP) to the Enterprise Architecture and Strategy Group (EASG), or by using the CMS POA&M database tool known as the CMS Contractor Integrated Security Suite (CISS) Tool. It also provides the instructions for Business Owners to enter CAP information into their copy of the CISS tool, if available, and how to upload to the CMS enterprise CISS database. Attachment A provides detailed instructions on how to complete the CAP Management Worksheet and also includes a blank CAP Management Worksheet. Attachment B provides instructions for Business Owners to obtain access to the CISS Tool. Attachment C provides instructions for identifying and managing findings that are infeasible to close using normal procedures. In addition, the Notification Memo template is provided for the Business Owner to use to submit the justification for closure to the Chief Information Officer (CIO)/Director of Office of Information Services (OIS).

.

TABLE OF CONTENTS

1. INTRODUCTION

The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing and administering an information security (IS) program to protect its information resources, in compliance with applicable laws, regulations, and Executive Orders. CMS employs the process defined by the Department of Health & Human Services (DHHS) in its *Information Security Program Plan of Action and Milestones (POA&M) Guide*, dated February 19, 2007. The *CMS Information Security (IS) Plan of Action and Milestones (POA&M) Procedure* is based on the DHHS guide and provides additional information and clarification.

1.1 Purpose

The *CMS IS POA&M Procedure* provides CMS IS management and Business Owners with the necessary information and instructions for developing, maintaining, and reporting their weaknesses in IS as it relates to a specific system.

1.2 Background

The *CMS IS POA&M Procedure* complies with the requirements prescribed by the Office of Management and Budget (OMB). Information is included to account for the emphasis that has been placed on formalizing the weakness mitigation process and ensuring weaknesses are appropriately prioritized for mitigation.

1.3 Scope

This document applies to all CMS Business Owners, and System Developer/Maintainers. Any personnel tasked with completing POA&M activities should read this document to become familiar with the CMS POA&M process.

1.4 How to Use this Document

This document was designed to be alignment with the DHHS POA&M Guide. Sections 2-5 and Section 7 of this document provide the CMS implementation of the DHHS guidance. Section 6 provides the instructions of how to manually submit the Corrective Action Plans (CAP) to the Enterprise Architecture and Strategy Group (EASG), or by using the CMS POA&M database tool known as the CMS Contractor Integrated Security Suite (CISS) Tool. It also provides the instructions for Business Owners to enter CAP information into their copy of the CISS tool, if available, and how to upload to the CMS enterprise CISS database.

2. POA&M OVERVIEW

A POA&M is a management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The CMS IS POA&M process will be used to facilitate the remediation of IS program- and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions;
- Defining roles and responsibilities for weakness resolution;
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses;
- Tracking and prioritizing resources; and
- Informing decision makers.

2.1 POA&M Purpose

The POA&M and its supporting processes enhance CMS' ability to identify, assess, prioritize, and monitor the progress of corrective actions pertaining to information security weaknesses found within *programs* and *systems*.[1] CMS uses the POA&M process to minimize security vulnerabilities, assist the Office of the Inspector General (OIG) in evaluating the agency's security performance, and through DHHS provides OMB with insight into the health and maturity of CMS' IS program.

Though the POA&M is expected to be a comprehensive plan, OMB assumes additional, more detailed project management plans exist for each corrective action item identified in the POA&M, and that the original source documents [e.g., Inspector General (IG) audit reports, risk assessments], in which weaknesses were first identified, are readily available. Thus, each POA&M weakness should be clearly traceable to its original source(s) and the documentation supporting the corrective actions should be maintained in the system security profile.

2.2 Security Program Maturity and the POA&M Process

Effective remediation of security weaknesses is essential to building a mature and sound IS program. Evidence of the proper implementation and use of the POA&M process is a critical element in the assessment of IS program performance by CMS OIG, DHHS, OMB and Congress.

2.2.1 System Funding

OMB requires each POA&M weakness to be linked to the capital planning and investment control (CPIC) process using unique project identifiers (UPI). The UPI, contained in the Exhibit 300 or 53, is submitted to OMB to request and justify the funding necessary to develop or maintain the system.[2] The UPI, from either the Exhibit 300 or 53, must match the UPI provided for the asset (e.g., system) and the associated POA&M. The consistent use of the UPI supports the correlation of the security costs associated with a program or system to its overall security performance.

[1] OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act,* August 23, 2004.

[2] OMB Circular A-11, *Preparation, Submission and Execution of the Budget* (updated June 2005)

When completing the POA&Ms and Exhibit 300s for major investments:

- Incorporate "Resources Required" for completing corrective actions and ongoing security costs into the total amount allocated for security.
- Include the funding represented in the 'Resources Required' POA&M field in Exhibit 300 documentation to support the overall increase in funding necessary to mitigate weaknesses.
- Ensure general weakness descriptions noted in CPIC documentation correspond to the weaknesses documented in the corresponding POA&M.

POA&Ms are used to assess the state of the CMS' IT Security and to aid in oversight of IT investments. OMB requires tying the POA&M to the budgeting process to evaluate the soundness of an investment. Systems that do not adequately address a plan for securing funding for mitigation of IT security weaknesses can be placed 'at risk' and lose funding. For major investments, OMB requires related POA&Ms to be cross-referenced through answers to questions when completing section II.B of an Exhibit 300. The response to all questions in this section of the Exhibit 300 should align with weaknesses reported in the POA&M that require funding.

For example, answers to question II.B.1(A) in the Exhibit 300 ("What is the total dollar amount allocated to IT security for this investment? Please indicate whether an increase in IT security funding is requested to remedy IT security weaknesses, specifying the amount and a general description of the weakness.") should link to the POA&M in the following manner:

- The total dollar amount allocated to IT security should include total required to mitigate potential weaknesses in addition to ongoing security costs.
- The increase in funding necessary to mitigate the weakness should match those listed in the 'Resources Required' column of the POA&M.
- Identification of the security weaknesses noted in the capital planning document should match those identified in the POA&M.

System-level POA&Ms are linked directly to the system budget request through the IT business case. Specifically, the UPI must be reflected on the POA&M for each system POA&M that is part of a capital asset plan and justification (Exhibit 300). This identifier will provide the link to agency budget materials. In addition, for those systems covered by an Exhibit 53 versus an Exhibit 300, the coverage of costs should be denoted as they were including in the Exhibit 53, including the UPI. This effort links the security costs for a system with the security management and performance of a system.

One of the key reasons for the creation and reporting of the POA&M to DHHS and OMB is the need to ensure security is integrated into the capital planning and budget process. Ordinarily, existing resources (staff and funding) will be used to correct a weakness. This is because the nature of the weakness and the corrective action warrants immediate attention.

When resources are required but not currently available to take corrective actions on identified weaknesses, however, they must be identified and recorded in capital investment documents and processes, i.e. the Exhibits 53 and 300. The POA&Ms are to be cross-referenced to the

corresponding Exhibits 53 and 300 line item numbers. According to the risk level assigned to the weakness, CMS does and will continue to place emphasis on resource identification and prioritization for any weakness that cannot be corrected until additional resources are provided, i.e. new money.

Actual dollars or staff hours needed to correct a weakness must be identified as part of the initial corrective action plan (CAP) in the "Resources" field of the POA&M. The Business Owner must specify whether funds will come from a reallocation of base resources (current hours or funding) or a request for new funding. CMS central office components must now also specify the Financial Management Investment Board (FMIB) investment number. (Place the FMIB # in the "Comments" field, if applicable.)

Resources identification: Early OMB guidance called for dollars or staff resources that are over and above current operating levels, e.g. the sample OMB provided POA&M worksheets with "None" in the "Resources" field for some items. Historically, CMS had only recorded resources where the dollars or FTEs did not come from current year funding (reallocation). As of 2004, CMS Business Owners must record person hours/FTEs and the dollars required to correct newly identified weaknesses.

2.2.2 Evaluation of the IS Program

OMB requires agencies to submit an annual FISMA report that summarizes the previous year's progress in establishing and maintaining an IS program. This report should include an IG evaluation of CMS' POA&M process. OMB uses these annual agency FISMA reports to assess the state of the Federal government's IS and generate a public report to Congress. In turn, the House Committee on Government Reform analyzes the information contained in each agency's annual FISMA report to derive the grades released in the Federal Computer Security Report Card as part of the President's Management Agenda (PMA). The PMA is part of the President's strategy for improving the management and performance of the Federal government.

2.3 Additional POA&M Benefits

Beyond its function as an authoritative IS management tool, the POA&M process has additional benefits, as evidenced in the sample list below.

- **Support Mission and Continuity.** By strategically addressing vulnerabilities in the POA&M, DHHS and CMS help ensure that organizational missions proceed without interruption or failure.
- **Allow Trending and Analysis.** The POA&M can be used as a historical data source for management reporting and business intelligence pertaining to the costs, effort, and time required to mitigate IS weaknesses. The type of weaknesses and the rate of reoccurrence can also be tracked. The POA&M provides the ability to conduct analyses at both system and program levels for both OPDIVs and the enterprise.
- **Support IT Business Cases.** A comprehensive POA&M, with accurate and reliable financial estimates, provides traceability and justification for additional security funds required to mitigate weaknesses and/or maintain the security of the program or system.

- **Maintain Institutional Knowledge.** A mature POA&M prevents reliance on one individual to retain and communicate information pertinent to a system or an entire program.
- **Facilitate Effective Communication.** The POA&M facilitates communication and coordination among various personnel such as the CMS Chief Information Officer (CIO), CMS CISO, Component Information System Security Officers (ISSO), budget personnel, Business Owners, and other program officials.

Each of these benefits provides DHHS and OPDIVs with greater monitoring capabilities over their IS program and increases the efficiency of IS management.

2.4 Roles and Responsibilities

POA&Ms are designed to be used predominately by Chief Information Officers (CIOs), Business Owners, System Developer/Maintainers, and Component Information System Security Officers (ISSOs) to track the progress of IT weakness corrective actions.

DHHS' guidance directs CIOs and program officials to develop, implement, and manage POA&Ms for all programs and systems that they operate and control (e.g., for program officials this includes all systems that support their operations and assets). The overall responsibility for the POA&Ms rests with the CIO, but others have significant roles as well.

The following POA&M roles and responsibilities outlined in this procedure are in addition to those designated in the *CMS Policy for Information Security* and other CMS policy and standards documents.

2.4.1 OIS Level

At the OIS level, the POA&M aids in the oversight of IS issues. The following have specific responsibilities related to the POA&M process:

- CIO
- Enterprise Architecture Strategy Group (EASG)
- CISO

2.4.1.1 Chief Information Officer (CIO)

- Assigns responsibility for oversight and management of the CMS POA&M.
- Is responsible for the transmission of agency progress in correcting weaknesses reflected in the POA&M and the results of independent IG inspections to DHHS.
- Reports to DHHS the results of CMS IS system and program reviews and progress in implementing the POA&M.
- Allocates proper resources to permit identification and remediation of weaknesses.

2.4.1.2 Enterprise Architecture Strategy Group (EASG)

- Oversees and maintains the CMS-wide IS program.
- Develops and maintains a comprehensive POA&M program.
- Coordinates and analyzes the POA&M process for improvements.
- Ensures the POA&M process is used to assess CMS-wide IS weaknesses.

2.4.1.3 Chief Information Security Officer (CISO)

- Assist in achieving and maintaining organizational compliance with CMS policy, standards, and procedures.
- Delegated authority from the CIO to accept risks that have a low risk level.
- Receive formal risk acceptance, review, and provide decision for internal justification for closure of findings that are infeasible to close using normal procedures.
- Ensures the POA&M process is used to assess CMS-wide IS weaknesses.

2.4.2 System Level

At the system level, the POA&M aids in the identification and evaluation of IS issues among individual systems. The following are the system-level roles and responsibilities related to the POA&M process:

- Business Owners
- System Developers/Maintainers
- ISSOs

2.4.2.1 Business Owners

- Work with Component ISSOs to develop, implement, and manage system-level corrective action plans for weaknesses in all systems that support their operations and assets.
- Update CMS management regularly (at the direction of the CIO or the management of their functional component) on the progress of weakness remediation efforts, enabling the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to DHHS and OMB.
- Requests proper resources to permit identification and remediation of weaknesses.

2.4.2.2 System Developers/Maintainers

- Develop and implement corrective actions that involve system modifications and enhancements.
- For the POA&M process, provide estimated dates of completion for these corrective actions.

2.4.2.3 Component ISSOs

- Work with Business Owners and System Developers/Maintainers to develop, implement, and manage CAPs for all information systems they own and/or operate.
- Ensure that the POA&M contains appropriate details, as required by OMB and DHHS.
- Conduct follow-up to verify a corrective action's status
- Update EASG at least quarterly, regarding the progress of the mitigation activities of each weakness.

3. WEAKNESS REMEDIATION PROCESS

Weakness remediation is the process whereby security vulnerability is identified, corrective actions are initiated, and the weakness is properly mitigated. This process is depicted in Figure 1, and the steps by which the process is carried out are described in greater detail throughout the remainder of this section.

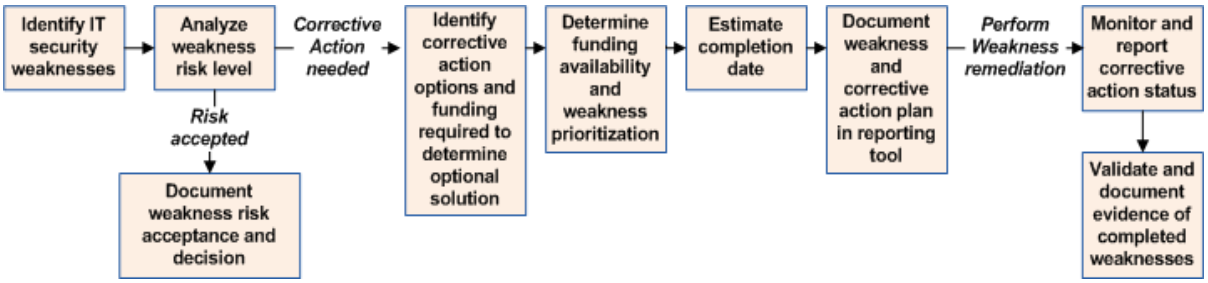

Figure 1. The Weakness Remediation Process

3.1 Identify Weaknesses

Weaknesses appropriate for tracking using the POA&M process can be identified proactively or reactively. Proactive weakness determination occurs when regular program and system reviews are conducted by the organization responsible and vulnerabilities are identified and/or documented. Reactive weakness determination indicates that the weakness was identified using audits or external reviews.

Sources of weaknesses may include findings from the following reviews:

- IG audits
- Government Accountability Office (GAO) audits
- Chief Financial Officer (CFO) reviews
- System self-assessments
- NIST SP 800-37 compliant security testing and evaluation (ST&E)
- IS program reviews
- Critical Infrastructure Protection (CIP) vulnerability assessments
- Risk assessments
- Penetration tests.

3.1.1 Weakness Types

All security weaknesses that represent risk to the security of a program or system and that require planned mitigation must be captured in the POA&M. To ensure a comprehensive POA&M process is in place, individual POA&Ms must be created for every program and system for which weaknesses are identified. Thus, two types of POA&Ms and associated weaknesses exist: program weaknesses and system weaknesses.

- Program Weaknesses. A program weakness impacts multiple systems as a result of a deficiency in the IS program. Program weaknesses are addressed separately from individual system weaknesses. Within the DHHS environment, a program POA&M will typically exist for each OPDIV.
- Program Weakness Example: The security policy is not updated in accordance with the most recent legislative guidance.
- System Weaknesses. A system weakness arises from a specific management, operational or technical control deficiency within a system. Each system weakness is entered individually on a system-specific POA&M.
- System Weakness Example: The system has not been certified and accredited or authorized to operate.

3.1.2 Risk-Based Exceptions

In some cases, a weakness may not be documented because a determination was made that the continued existence of the weakness is an acceptable risk. Such a determination must be certified by the Business Owner and documented accordingly. Section 4.3 discusses closing a finding under these circumstances.

3.2 Define Mitigation Method

Multiple weakness mitigation methods often exist. Such methods should be analyzed for their ability to fully resolve the weakness in the most efficient manner. The cost for each option should be estimated and analyzed to determine short- and long-term solution options.

3.3 Determine Funding Availability

The cost of weakness remediation activities must be determined and included in program and system POA&Ms. Additionally, the availability of funding required to mitigate weaknesses must be evaluated. Three funding scenarios exist in support of weakness mitigation efforts.

- Current resources exist that may be allocated to mitigate identified weaknesses. (This is the scenario most commonly adopted because the weaknesses need to be addressed in the near term.)
- Resources exist but must be reallocated to support weakness mitigation.
- Additional funding must be requested and allocated.

If new funding is required, the existing capital planning process should be relied upon to request and receive the necessary funds. Funding requests for system security costs typically occur

through the creation of Exhibit 300s and 53s. The OPDIV remains responsible for continuous progress towards weakness mitigation.

3.4 Prioritize Weaknesses

FISMA guidance requires CMS to prioritize POA&M weaknesses to ensure the most critical security weaknesses and/or the weaknesses identified on systems with the greatest potential impact to the organization's mission are addressed first.

Resource limitations often prevent the Business Owner from obtaining the resources necessary to mitigate every identified weakness within the same time period. The careful prioritization of weaknesses helps to ensure that critically important weaknesses are allotted resources within a time period proportionate to the risk associated with the vulnerability or system.

Rank-ordering corrective actions to address weaknesses according to specific criteria are key to effective prioritization. Documented rank-ordering criteria enable the Business Owner to prioritize corrective actions in a standardized fashion against factors that are specific to the CMS operating environments. Criteria against which weaknesses may be prioritized include:

- Risk level of weakness and/or risk impact level of system as categorized according to CMS System Security Level (*www.cms.hhs.gov/informationsecurity* under "Standards");
- DHHS security initiatives;
- Specific security control implementation;
- Cost effectiveness of implementing the corrective action; and
- Length of time since the weakness was identified.

Basic weakness prioritization focuses on two criteria: system categorization and weakness risk level.

According to FIPS 199, a system should be categorized as low, moderate, or high based on the confidentiality, integrity, and availability of the information it stores, processes, or transmits. System characterization should be determined in the system's risk assessment according to the criteria articulated in the *CMS Security System Security Levels.* All CMS FISMA reported systems have been so classified by information category.

The resulting system categorization, also known as the risk impact level, should then be used to help identify those weaknesses that require immediate attention. For example, weaknesses associated with a system classified as having a high risk impact level may pose a greater risk, if not mitigated in a timely manner, in comparison to a low risk impact level system possessing the same weakness.

3.5 Assign Estimated Completion Dates

The estimated date of completion for each weakness must be based on realistic timelines that allow for resources to be obtained and associated steps to be completed. The completion date should be based on the outcome of prioritization decisions and resource availability.

3.6 Document the Corrective Action Plan (CAP)

OMB mandated a POA&M format to provide a consistent baseline of required and standardized information. This structure improves the ability of IS stakeholders to easily locate information and organize details for analysis. The format includes a location for the identified system or program weakness, any associated milestones and necessary resources required. Specific information regarding each individual component of the required POA&M format is discussed in Section 6.

3.7 Monitor and Report POA&M Activity

The information in the POA&M should be maintained continuously and a quarterly status report must be provided to communicate overall progress to DHHS in identifying and mitigating weaknesses. The format of the quarterly CMS POA&M summary status report is shown in table 1 below. The one represented in the DHHS Procedure is for their report to OMB. The table below is how CMS reports to DHHS.

Table 1. Format of Quarterly Summary Update to DHHS

Quarterly POA&M Updated Information	Programs	Systems
Total number of weaknesses identified at the start of the quarter		
Number of weaknesses for which corrective action was completed on time (including testing) by the end of the quarter		
Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled		
Number of weaknesses for which corrective action has been delayed, including a brief explanation for the delay		
Number of new weaknesses discovered following the last POA&M update and a brief description of how they were identified (e.g., agency review, IG evaluation, etc.)		

CMS is expected to update its POA&M and POA&M summary report continuously and be prepared to submit them at the request of the DHHS Chief Information Security Officer (CISO), within seven to fourteen business days in advance of the OMB quarterly deadlines. The POA&M Summary Update Report is prepared by the Division of IT Policies, Procedures and Audits, Enterprise Architecture & Strategy Group (EASG), Office of Information Services (OIS).

3.8 Validate Weakness Completion

OMB's FISMA reporting guidance recommends that weaknesses should be considered "Completed" only when they have been fully resolved and the corrective action has been tested.

Testing completed weaknesses demonstrates that the program vulnerability or system control has been adequately addressed and proven effective. This step should be explicitly incorporated into the weakness mitigation process and documented accordingly.

3.9 Retire and Transfer Weaknesses

OMB M-04-25 advises that weaknesses that have been mitigated for over a year should no longer be reported in the POA&M. CMS ages off any weaknesses that have been "Completed" for at least 12 months.

The transfer of POA&M weaknesses from one FISMA system to another must be clearly traceable and justified. Upon documentation within the POA&M, weaknesses may only be removed due to transfer to another program- or system-level POA&M or retirement by the 12 month rule above.

4. POA&M COMPONENTS AND FORMATTING

Each program or system-level POA&M is formatted using the same required fields, which contain information about the weakness and its associated remediation activities. This section describes the content and formatting for each of the prescribed fields, listed in Table 2, inclusive of both OMB and DHHS requirements.

Table 2. POA&M Field Descriptions

Field Heading	Contents—How to Complete
Weakness Identifier	The weakness identifier is used to track weaknesses from quarter to quarter.
Weakness Description	A weakness represents any program- or system-level information security vulnerability that poses an unacceptable risk to the confidentiality, integrity, or availability of information.
Point of Contact	The point of contact (POC) is the organization and/or position title within the Department or OPDIV that is responsible for weakness mitigation.
Resources Required	Resources required include the funding or man-hours necessary for mitigating a weakness. The type of funding (new, existing, or reallocated) should be noted.
Scheduled Date of Completion	The scheduled date of completion should be based on a realistic estimate of the amount of time it will take to organize the resources necessary to implement and test the completion of the corrective action.
Description of Milestone	Milestones outline the high-level activities necessary to fully mitigate the weakness.
Changes to Milestones	At a minimum, a change to a milestone should indicate the new estimated date of completion if the original milestone date cannot be met. Actual milestone completion date should be included within this field.
Identified in CFO Audit or Other Review?	This field must note the review type, reviewing organization, and the publication date of the document that first identified the weakness being addressed.
Status	This field is used to report the status of the weakness. Options are limited to Completed, Ongoing, or Delayed.
Weakness Comments	This field is used to document additional detail or provide clarification, and must be used if a weakness lapses into delayed status to explain the reason(s) for the delay.
Weakness Severity	The weakness severity field is used to categorize each weakness based on the risk it poses to the organization's overall security. The weakness severity categories are limited to significant deficiency, reportable condition, or weakness.

Please note, once the CMS has submitted the initial POA&M, no changes can be made to the data in the following fields:

- Weakness Identifier;
- Weakness Description;
- Scheduled Date of Completion;
- Description of Milestone; and
- Identified in CFO Audit or other Review.

4.1 Weakness Identifier

Each POA&M weakness is assigned a weakness identifier. This identifier is used to track weaknesses from quarter to quarter. The numbering schema used to generate the weakness identifier for a system consists of the name of the associated system, the quarter and FY during which the weakness was first recorded on the POA&M, and a sequence number. A program weakness identifier uses the program name in lieu of a system name. See Figure 2 for a sample system weakness identifier.

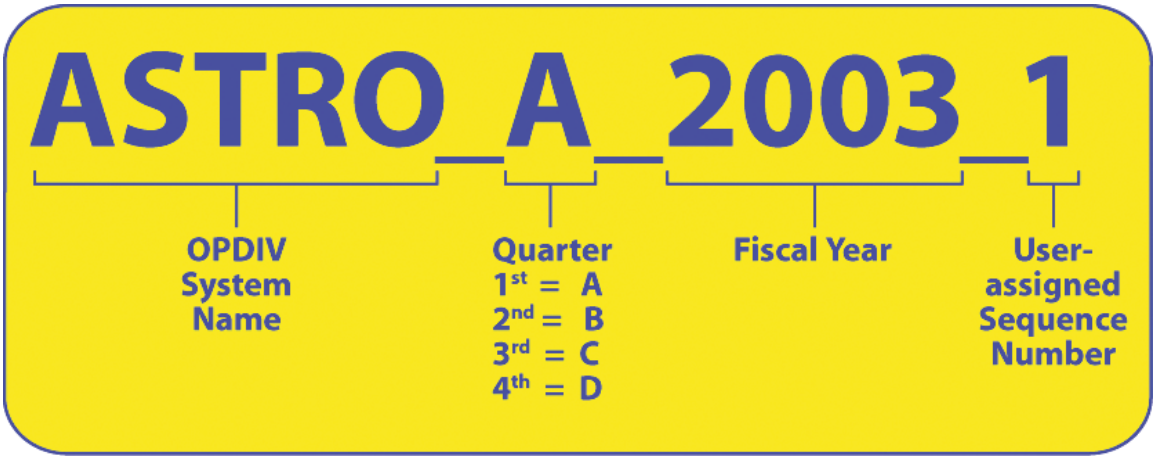

Figure 2. Sample System Weakness Identifier

In the sample above, 'ASTRO' represents the CMS system name or acronym. The letter 'A' represents the quarter in which the weakness was first identified and entered on the POA&M. The number '2003' represents the FY in which the weakness was identified and submitted. The value '1' represents the numerical order in which this weakness was entered on the POA&M for the ASTRO system.

4.2 Weakness Description

The term 'weakness' refers to any program- or system-level IS vulnerability that poses a risk to the confidentiality, integrity, or availability of CMS' information. Weaknesses represent the

gaps between the current program or system status and the long-term program or system security objectives.

When reporting weaknesses, consideration must be given to the level of detail revealed in the POA&M. Detailed descriptions are neither necessary nor recommended; however, sufficient data is required to enable appropriate oversight and tracking, demonstrate awareness of the weakness, and articulate specific actions initiated to address the weakness. Sensitive information should never be included in POA&Ms due to the risk of system vulnerability exposure and/or exploitation it enables. General wording consistent with that found in GAO and IG reports should be used to complete the POA&M. When necessary, additional details may be provided in the "Weakness Comments" field.

Table 3 contains examples of weakness descriptions that are improperly phrased and subsequent suggestions for revision to create acceptable entries.

Table 3. Unacceptable vs. Acceptable Wording of Weaknesses

Less Appropriate	Reason Improvement is Needed	More Appropriate
Passwords are easily guessed	Sensitivity level	System does not adhere to password policy
Telnet port open, allowing access by outside users	Sensitivity level	Unnecessary services are enabled
Penetration test to be conducted	This is a milestone that will mediate a weakness	Security reviews to detect system weaknesses not conducted on an periodic basis
Additional operational controls needed	Description reflective of a milestone, not the overarching weakness	Background investigation procedures require review

EASG does not advocate "roll ups" of findings into more global weaknesses. This provides more direct accounting of each finding. It is recommend that each finding be recorded, but CMS has extended the business owners the flexibility to roll up some findings into weaknesses when it makes sense to do so and as long as the guidance above regarding traceability back to the individual finding is preserved.

Weakness "Roll-Ups": Under the CMS POA&M reporting CISS tool, individual findings may be rolled-up into a weakness for such reasons as the same actual root cause or systemic problem. In these situations, the individual finding numbers will be captured in the POA&M "Identified" field. In addition, the CISS tool will actually track CAPs by finding; by source of review. Details are always available in the CMS enterprise CISS tool database.

4.3 Point of Contact

A POC must be identified and documented for each weakness reported. The POC is the position/role (e.g., Component ISSO, Business Owner) responsible for resolving the weakness. Since personnel in these positions may change, using specific POC names is not recommended.

Useful Tips:

- Avoid listing personnel names and phone numbers for the POC.
- Ensure that a POC is listed for all weaknesses.
- Include more than one POC for each weakness if necessary.
- Ensure that the identified POC is aware of and accepts the responsibility for mitigating the weakness.

4.4 Resources Required

Weakness correction requires resources; the type and amount of which will vary. If existing government personnel are assigned to correct the weakness and no new funding is required, the POA&M should identify the amount of time it will take to complete the corrective action (e.g., 60 hours) and that it is performed by current staff. The resources required estimate must be based on the total resources needed to fulfill all the milestones necessary for weakness correction. The type of funding (new, existing, or reallocated) should be noted in addition to the dollar amount and/or man hours. Specific information related to non-funding obstacles and challenges to resolving the weakness (e.g., lack of personnel or expertise, development of a new system to replace vulnerable legacy system) should be included in the 'Weakness Comments' field.

Useful Tips:

- Identify resources for mitigating each weakness.
- Ensure that resources are estimated as man-hours or monetary value.
- Identify monetary funding as "new funding," "existing funding," or "reallocated funding." These descriptors can also be applied to staffing requirements (e.g., 'new staff' or 'existing staff').

4.5 Scheduled Date of Completion

The scheduled date of completion should be determined based on a realistic estimate of the amount of time it will take to allocate the required resources, implement the corrective action(s), and complete all associated milestones. Draft documents are not considered evidence of completion by OMB or Congress. It is therefore important to incorporate review and finalization process steps into the overall completion timeline.

The scheduled date of completion should include the month, day, and year, and may not be changed after initial POA&M entry; progress toward completion is tracked through milestones. If the time to correct the weakness extends beyond the original scheduled date of completion, the status of the weakness must be changed to 'delayed,' and reasons for the delay should be noted in the 'Weakness Comments' field. A revised scheduled date of completion must be recorded in the 'Changes to Milestones' column and reasons for the change must be noted in the 'Comments' field.

Useful Tips:

- Define scheduled dates of completion for all weaknesses.
- In developing scheduled completion date, incorporate adequate time for development, review and finalization of documentation.
- Ensure that the initial scheduled date of completion is not changed if the weakness is mitigated either before or after the planned date.

4.6 Description of Milestone

Milestones are the specific, action-oriented steps necessary to mitigate a weakness. The number of milestones articulated per weakness should directly correspond to the number of steps or corrective actions necessary to fully address and resolve the weakness. Each weakness must have at least one corresponding milestone with an anticipated completion date. The milestone completion date identifies the allotted time reserved to address the individual milestone and helps place milestones in a logical order.

Milestones should effectively communicate the major steps that will be performed to mitigate a weakness. For example, appropriate milestones for a weakness like, "Identification and authentication processes need to be more stringent" would read:

- Evaluate methods for strengthening identification and authentication
- Develop procedures to standardize accepted authentication process
- Implement appropriate authentication process.

Once milestones and completion dates are entered in this column, changes *cannot* be made. If estimated milestone completion dates change, the new expected date must be recorded in the 'Changes to Milestones' column and reasons for the change must be noted in the 'Comments' field. 9

Useful Tips:

- Develop milestones using actionable words and phrases (e.g., identify, incorporate and review); limit milestone to no more than one task.
- Ensure the last milestone schedule completion date does not exceed the schedule completion date for the overall weakness.

4.7 Changes to Milestones

The "Changes to Milestones" field is designed to accommodate fluctuations in the availability of resources, periodic reprioritization of activities, and unanticipated delays that organizations regularly experience. If a situation exists that prevents a milestone and/or the overall corrective action from being completed as originally estimated, the new or revised milestone and/or anticipated date of completion should be identified in the "Changes to Milestones" field. No changes can be made to the original estimate in the "Scheduled Date of Completion,' or 'Description of Milestone,' fields. As with all completion dates in the POA&M, the new

milestone completion date should include the month, day, and year of estimated completion. An explanation for the revised milestone and/or milestone completion date must be entered in the "Comments" field.

4.8 Identified in CFO Audit or Other Review?

This field should be used to list the method by which the weakness was originally identified. Section 3.1 outlines the most common sources and methods of identifying POA&M weaknesses. When recording the weakness source, ensure the information includes both the type of review and the date—including the month and year—on which this review was conducted or published.

Useful Tips:

- Identify sources for all weaknesses.
- Ensure the review type and the review's month and year are documented.
- Include all weaknesses identified in annual IG FISMA evaluations in corresponding program- or system-level POA&Ms.

4.9 Completion Date

This field represents the actual date the last corrective action milestone was completed for the weakness in a month, day, year format.

4.10 Status

Statuses—Completed, Ongoing, or Delayed—should be assigned to each corrective action to denote progress toward mitigation. Identifying the current status of a corrective action demonstrates that the POA&M is a dynamic management tool and part of an ongoing monitoring process.

- **Completed**. This designation is used only when a weakness has been fully resolved and the corrective action has been tested. When listing items as 'Completed,' the date of completion should also be noted. Upon completion, the weakness will remain reportable for one year. After one year, the weakness should be archived in an effort to maintain only reportable weaknesses on the POA&M.
- **Ongoing**. This status indicates that the weakness continues to be mitigated consistent with the associated scheduled completion date.
- **Delayed**. If a weakness lapses into 'Delayed' status by surpassing the original scheduled date of completion, due to unforeseen events and/or scheduling conflicts, an explanation must be provided in the 'Weakness Comments' field. If the scheduled date of completion has been revised and documented in either the 'Changes to Milestone' or 'Weakness Comments' field, the weakness is still considered to be 'Delayed' because it exceeds the original scheduled date of completion.

Useful Tips:

- Indicate status as “Completed,” “Ongoing,” or “Delayed” only.
- Keep abreast of weaknesses mitigation activities in order to ensure the status accurately reflects the environment at that particular point in time.

4.11 Weakness Comments

The “Weakness Comments’ field provides an area in which further detail and clarification can be added. This field is often used when modifications have been made to specific corrective actions. Also, this field may be used to provide explanations and further insight into challenges encountered during weakness mitigation and dependencies that may impact the completion of these activities. When the scheduled date of completion has been exceeded and the weakness is therefore considered “Delayed,” this field should be used to address the reason for the delay.

The name of the application within a FISMA reported Major Application should be clearly stated in the comments field, unless this information is reflected in another column of the POA&M such as the weakness description. For example, if the weakness applies to the Enrollment Database (EDB) application within the FISMA-reported Medicare Beneficiary Enrollment System, the EDB application should be clearly stated in the comments field.

4.12 Risk Level

The “Risk Level” field has been added to the POA&M to denote the determined potential impact of a weakness on the system, data, and/or the program. An appropriate risk level should be assigned to each weakness based on the potential impact and threat likelihood of exploitation of the weakness. Risk level definitions can be designated as High, Medium or low. Except for self reviews, most evaluation reports assign risk levels to weaknesses (findings).

4.13 Weakness Severity

This field will always be annotated as “Weakness”. The OMB and HHS Procedures also provide for the categorization of weaknesses into “significant deficiency” or “reportable condition.” Experience has shown these categories almost never apply, but should a Business Owner or a System Develop/Maintainer feel the severity of a weakness is such that it rises to these levels, they should consult with OIS/EASG staff.

5. FORMALIZING THE POA&M PROCESS

A comprehensive POA&M process creates a repeatable cycle that effectively and efficiently corrects weaknesses. This process includes:

- Formal process development;
- Ongoing identification and review of POA&M inputs;
- POA&M documentation development and reporting;
- Weakness remediation;
- Information verification; and
- Post-remediation improvement efforts.

5.1 Formal Process Development

The POA&M policies and procedures, in conjunction with prescribing the creation and maintenance of POA&Ms, ensure consistent application and accountability. Through this process, specific roles and responsibilities are assigned and adequate training is provided to aid personnel in the understanding and implementation of their assigned roles. Developing prioritization criteria further ensures that weaknesses are corrected within specified time frames, and resources are assigned consistent with the associated weakness risk.

5.2 Ongoing Identification and Review of POA&M Inputs

Identifying and monitoring potential POA&M input sources are integral to the formalization of the POA&M process. All sources that may identify a program- or system-level weakness should be reviewed on a periodic basis. This review will enable the timely incorporation of all known IS vulnerabilities associated with information programs or systems used and operated by the CMS or any of its contractors. Weaknesses must also be evaluated for risk acceptability; regular discussions should take place with management regarding the execution and documentation of risk-based decisions. POA&Ms must be created for **ALL** weaknesses that require remediation.

5.3 POA&M Documentation Development and Reporting

Developing and maintaining POA&M documentation, combined with periodic reporting, is evidence that the POA&M process has been formalized. Each weakness requiring corrective action must be captured, consistent with the standards and required elements set forth by OMB, DHHS, and CMS. It is imperative that reporting procedures are strictly followed, including the development of quarterly and annual reports furnished to DHHS for submission to OMB.

Business Owners must perform the following actions:

- Capture all weaknesses for the POA&M through the CISS tool or the POA&M manual reporting process.
- Appropriately resource corrective actions.
- Manage and document corrective actions.
- Report status at least quarterly to EASG until acceptance and closure by EASG.

There are two methods for capturing information for POA&M reporting. CMS has developed a database and supporting tool, CISS, to automate the CMS POA&M corrective action and reporting process. The CISS tool was implemented in FY 2005 at the Medicare Contractor sites to allow the contractors to track their individual findings and submit them to CMS for inclusion in the enterprise CISS database for overall POA&M tracking. For all other CMS systems, a manual reporting process is in place using the CAP management worksheet. EASG reviews all the submissions and enters them into the enterprise database. CMS is in the process of migrating all FISMA systems to the CISS tool to fully automate the POA&M reporting and maintain an enterprise CISS database for recording details and tracking corrective actions for all findings before uploading into the DHHS POA&M tool, ProSight.

Again, the goal is to generate reports by FISMA system and/or Medicare contractor. Detailed information on the CMS POA&M Reporting and CAP submission processes (manual or automated) refer to Section 7 of this document.

5.4 Weakness Remediation

Timely mitigation of existing weaknesses, combined with the identification and mitigation of new weaknesses indicate that an operational POA&M process is in place. Prioritizations of such weaknesses reinforce the overall maturity of such a process. As mandated through FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, it is especially important to utilize the *CMS Policy for the Information Security Program* and the associated IS standards in the *CMS Information Security Acceptable Risk Safeguards* on www.cms.hhs.gov/informationsecurity since they contain the foundational controls from which all systems are to be continuously monitored.

5.5 Information Verification

A mature POA&M process includes steps to validate the mitigation of weaknesses and ensures the accuracy of reported information. Estimated completion dates for weaknesses and milestones should be reviewed following the completion of a weakness. When the finding is a result of in independent evaluation, the reviewer reviews the closed findings and determines if they have met the requirement, either by retesting or accepting the submitted documentation as proof of closure. All closed finding must be supported by documentation and the Business Owner must maintain this documentation in the system security profile along with the other IS artifacts, e.g. IS Risk Assessment (IS RA), System Security Plan (SSP). Validation should be thorough enough to ensure the integrity of the information placed within the required fields and maintain consistent submission dates during each quarterly reporting period.

5.6 Post-Remediation Improvement Efforts

Over time, information collected from actual POA&Ms, and from the process in general, will be used to advance weakness mitigation effectiveness. CMS has and will leverage lessons learned through mitigation to establish efficient procedures in order to avoid potential weaknesses and develop an improved IS program posture.

6. CMS POA&M REPORTING AND THE CAP PROCESS

EASG, OIS is the control point for accounting and tracking to closure all identified findings (potential weaknesses) from all sources of IT reviews of CMS systems and the IS Program. Any identified IT finding must be entered into the POA&M reporting and corrective action process. EASG assigns responsibility and facilitates the creation of a CAP in the POA&M format by FISMA system.

Once the final report for an audit, review, evaluation, assessment or systems test and evaluation (ST&E) is completed, the auditor, project officer (PO)/Government Task Leader (GTL) and/or

testing contractor will provide EASG with a copy of the report. EASG will coordinate with Business Owners to ensure they are aware of the need to submit a CAP for each finding.

Following issuance of the final report, the CAP Management Worksheet and Instructions (Refer to Attachment A for the CAP Worksheet Requirements) are sent to the Business Owner and CAPs must be submitted to EASG within 30 calendar days. All open findings in the final report must be addressed with a CAP. The Business Owner may enter the CAP directly into their FISMA system instance of the CISS tool, if available. For those systems with CISS tool access, they will provide EASG with monthly updates of their CISS file. Detailed instructions can be found in the CISS User's Procedure (www.cms.hhs.gov/informationsecurity under "Guidance"). EASG staff will review the CAPs to ensure the reporting instructions have been followed and the vulnerabilities in the report are addressed.

If needed, EASG will schedule a meeting with the Business Owner and/or System Developer/Maintainer for the system to discuss any questions or issues that they may have with regard to the requirement for a CAP or the format for submission. For example, meetings may be necessary to allocate findings to General Support Systems versus Major Applications.

During the meeting, EASG will affirm the due date for the CAP to be submitted to EASG (if the CISS tool is unavailable to the Business Owner) or entered into the CMS CISS tool following approval of the CAP by the Business Owner. Any EASG review of the CAP will focus on ensuring that all essential elements of information are included, not necessarily on the accuracy of the CAP to address the individual finding. The adequacy of the CAP to address the finding(s) is the responsibility of the Business Owner.

NOTE:

For SAS-70 and CFO EDP audits – The Office of Financial Management (OFM) is in charge of the review process. OFM instructions require CAPS from contractors on all findings after a final audit report is received. Each individual finding is tracked to completion through the OFM UCAP process and OIS or Center for Medicare Management (CMM) oversight. CMM recommends closure of all SAS-70 and CFO EDP Audit findings to OFM for Fiscal Intermediaries, Carriers, and Medicare Administrative Contractors (MACs). The OIS Enterprise Data Center Group (EDCG) makes similar recommendations for the Medicare Data Centers. Closure should be always based on either a subsequent audit/review or a verification of closure documentation by auditors or CMS staff in Central Office (CO) or the Consortia Contract Management Officer in the regions. All SAS-70 and CFO EDP audit findings must be recorded in the CISS tool and reported as part of the CMS POA&M.

CO CFO EDP and FISMA audits– EASG assigns responsibilities on findings, records details and tracks CAPs in the CMS POA&M database. These findings are entered quarterly into the DHHS ProSight POA&M tool.

System Security Testing (e.g., JANUS and Mitre) at Central Office – results are entered on the CAP Management Worksheet (Attachment A) by FISMA reported systems as part of the testing report. Business Owners provide CAPs to EASG within 30 days of receiving the CAP

Management Worksheet. Individual CAPs are tracked by EASG in the CMS enterprise CISS database and report them quarterly to DHHS using the ProSight POA&M tool.

Certification & Accreditation (C&A) and Authority To Operate (ATO) Actions – all required actions are reviewed by EASG and cross-checked to ensure these are not findings identified by a prior review's or security test. All verified CAPS are entered by EASG into the CMS POA&M by FISMA system.

Business Owner Identified Weaknesses – those risks identified by the Business Owner through the risk assessment process (part of the CMS Integrated and System Life Cycle Framework, www.cms.hhs.gov/SystemLifeCycleFramework) must be mitigated. These are to be entered on the POA&M CAP Management Worksheet and submitted to EASG or , if available, entered into their instance of the CISS database. An example is a weakness identified as part of annual security control testing.

6.1 Quarterly Reporting on CAPS

EASG will make quarterly requests for updates of the CAP Management Worksheet for those FISMA systems without CISS tool access. However, by the first of every month, all the new Findings, Weaknesses, and Actions Plans (Open and Closed) for all other FISMA systems must be entered into their instance of the CISS tool. Any outstanding Action Plans must be updated and a validation test on the database must be performed per the CISS Users Procedure. If errors are found, the errors must be corrected before a submission file can be created. Once the database has passed the validate test, a submission file can be created and forwarded to the EASG POC. EASG will perform a validate test on the submission file to ensure that there are no errors in the file. If errors are detected the Business Owner of that FISMA system file will be contacted and the error(s) must be corrected and a new submission file must be created and resubmitted to EASG immediately. Once the submission file passes the validation test, EASG will import the submission file in to the CMS enterprise CISS database. Subsequently, EASG will submit all POA&M reporting to DHHS using ProSight

If updates are not received in a timely matter or if the findings are not being addressed, EASG will alert the CIO. EASG may also schedule monthly meetings with the Business Owners and/or System Developers/Maintainers and their staff to ensure that the findings are addressed.

6.2 Requirements to Close A Finding

High and Medium Risk Findings: CMS does not allow Business Owners to accept risk for High or Medium Findings. They **must** be mitigated. The Business Owners must make every attempt to close all findings. Once the CAP has been implemented, the Business Owners shall forward all supporting documentation that show evidence that the CAP is completed to EASG, as well as keep copies in their system's security documentation file.

In the event a vulnerability cannot be fully resolved, the Business Owners must ensure that adequate security controls have been put in place to reduce the risk to low. Once the security controls have been put in place, the Business Owners must submit all supporting documentation

to EASG to verify that the security controls have been implemented. Low risk findings may be closed based on an approved risk acceptance memo (Attachment C - .Internal Justification for Closure of Finding Template and Instructions). The Business Owner will need to submit the memo to OIS for approval. In the memo, the Business Owners will need to explain the reason for accepting the risk including a description of any compensating controls used to lower the risk.

For all risks that are accepted the Business Owner must:

- Address them in the system's SSP and/or IS RA.
- Review and re-submit the Justification for Finding Closure to OIS if the controls put in place are still valid and appropriate, e.g., upon re-certification of the system.
- Review the accepted risks when a major change to the system has been performed, and
- Retain copies of the approved justification memo as part of the system security documentation file.

6.3 Verification of Completed "Closed"

In the CISS database, many findings are shown completed "closed pending." This is done to record completion of a CAP prior to CMS or independent auditor verification, necessitated by the fact that many of these items cannot be validated for months after the reported closure dates (for example during follow-on audits). To do so otherwise would grossly overstate the number of non-completed or "delayed" findings.

EASG aggressively manages the POA&M process and uses various activities to validate actual closure including CMS (Central Office and CCMS staff) desk review and/or on-site validation, auditor re-reviews and follow-on audits/evaluations. Because of timing of the validations, (for example 912 evaluations don't begin until late summer) it is not uncommon to have many findings in the completed "pending verification" status at any given time.

7. CONCLUSION

The POA&M process provides significant benefits to both CMS and DHHS. It is a dynamic management tool useful for ongoing efforts to address programmatic and system-specific vulnerabilities. It assists in essential decision-making activities, facilitating and helping to ensure the oversight and mitigation of security weaknesses and the cost-effective use of mitigation resources.

To function effectively, POA&Ms must be continually monitored and diligently updated. A mature POA&M process requires that the knowledge and efforts of each CMS component are sustainable over time, independent of any organizational and personnel changes. An effective POA&M captures each of these changes completely and concisely.

ATTACHMENT A: CAP MANAGEMENT WORKSHEET

The following instructions explain how the CAP Management Worksheet should be completed. The initial update to the Form will require more information then the monthly updates/status reports. Information must be entered in columns 2, 3, 4, 5, 6, 8, 9 and 10 for each reported finding/action item for the initial submission. Once the initial CAP Management Worksheet has been completed and submitted to EASG, no changes may be made to the data in columns 1, 2, 3, 4, 5, 6, and 8. Only columns 7, 9, 10 and 11, may be updated for the monthly reporting. When a finding /action item is closed, either during the initial or monthly submission, specific documentation for verification is required along with the submission.

Column 1 – **Weakness Tracking Number.** This column is for the tracking number that is assigned to the weakness when entering the weakness into CISS Tool.

Column 2 – **Weakness**. The description of the detailed finding/action item identified in an Authority to Operate (ATO) or Certification & Accreditation (C&A) memorandum will be pre-filled in this column. Sensitive descriptions of specific findings are not necessary, but sufficient data must be provided to permit oversight and tracking**. Example of a Weakness would be: The System's System Security Plan (SSP) and Risk Assessment (RA) are out dated.**

Column 3 – **POC**. Identity the name of the Point of Contact (POC), position/ title and organizational entity that the component head will hold responsible for resolving the finding./action item **Must be a CMS staff.**

Column 4 – **Resources Required**. Estimated staff time in hours required to resolve the finding/action item. Identify any cost (e.g. contract costs) associated with resolving the finding/action item and identify the FMIB number for the investment. This column cannot be left blank or equal 0.

Column 5 – **Scheduled Completion Date.** Scheduled completion date (mm/dd/yy) for resolving all the milestones the finding/action item. Please note that the initial date entered may not be changed. If a finding/action item is resolved before or after the originally scheduled completion date, the CMS Business Owner [or designee] should note the actual completion date in Column 9, "Completion Date." EASG recommend the following four dates as the scheduled completion dates for Column 5: January 2, 20xx, April 2, 20xx, July 2, 20xx or October 2, 20xx.

Column 6 – **Milestones with Completion Dates.** Key milestones with completion dates must be entered into this column. A milestone will identify specific requirements or key steps to correct an identified finding/action item. If the finding/action item has two or more identified issues or elements contributing to the overall finding/action item, the milestones and completion dates must be comprehensive enough to address all elements of the finding/action item. Please note that once entered on the POA&M form from the CAP Management Worksheet, the initial milestones and completion dates may not be altered. If there are changes to any of the milestones and /or scheduled completion dates the component should note them in the column 7, "Changes to Milestones" and provide a reason for the change in column 11 "Comments." Example of Milestones would be: Milestone 1: Update System's SSP Milestone 2: Update System's RA.

Column 7 – **Changes to Milestones.** This column only needs to be completed if the CAP cannot be completed by the Milestones Completion Date from Column 6 or the Scheduled Completion Date in Column 4 cannot be met. This column would include new completion dates for particular milestones or scheduled completion date. The reason for the change must be recorded in Column 11 "Comments".

Column 8 – **Identified.** The source of where the finding/action item was found and the associated finding numbers are entered in this column. Example: ATO-001, 2006 CFO Audit-005.

Column 9 – **Completion Date.** The date that all the milestones have been completed.

Column 10 – **Status.** The only entries permitted are "on-going", "delayed" or "completed." If "delayed", an entry must be made in Column 7 "Changes to Milestones" with new completion dates for the particular milestone. The reason for the change must be recorded in Column 11 "Comments".

Column 11 – **Comments.** Record a brief summary of the work accomplished during the reporting period. An entry is also required if a scheduled completion date or milestones date is missed (record the reason) or if the finding/action item has been corrected and all work is deemed "completed" (record the date of completion). Record any additional details or clarification for any previous entries as well as the application/system name related to the finding in this field.

Column 12 – **Risk Level.** This is the risk level [High, Medium, or Low] assigned to the finding by the reviewer and cannot be changed by the Business Owner or System Developer/Maintainer. Any findings without a designated Risk Level will be assigned by EASG.

Column 13 – **Weakness Severity.** The severity level is "Weakness".

FISMA System Name:

CAP Management Worksheet

1 Tracking #	2 Weaknesses	3 POC (Must be CMS Staff)	4 Resources (Must be in Hours or Dollars)	5 Scheduled Completion Date	6 Milestones Completion Dates	7 Changes to Milestones	8 Identified	9 Completion Date	10 Status	11 Comments	12 Risk Level	13 Weakness Severity
	-											

Date:

ATTACHMENT B: PROCEDURES FOR OBTAINING ACCESS TO CISS

1. Each FISMA System Family Business Owner shall designate one primary user and one backup to be responsible for entering and tracking all FISMA status requirements including weaknesses for all applications within the system family. This authorization will be in the form of an e-mail to the Director EASG/DITPPA with a cc: the Director EASG and the CISO.

2. The authorized users for the FISMA System Family will be scheduled by EASG to attend CISS Training before the CISS Tool is installed on their desktop.

3. Each authorized user must submit a service request to the CMS_IT_Service_Desk to have the Tool installed on their desktop.

4. The CMS_IT_Service_Desk will verify the user's access with EASG POC prior to installation.

5. The EASG POC will maintain the authorized list of CISS users and will validate the list no less than annually. All additions/deletions/changes in the authorized users must be submitted via email by the FISMA System Family Business Owner to the EASG POC with the above cc:s.

6. Prior to entering data via the CISS tool, EASG will provide a copy of the CISS Database populated with the current information for the designated FISMA System Family only. This will be the business owner's repository to maintain and track the FISMA status of the System Family and can only be accessed through the CISS Tool by the authorized user(s). Included in maintaining the FISMA status for the System Family, each FISMA System Family Business Owner must establish a means for the application business owners to report the status, including all new or on-going weaknesses, of each application directly to the CISS authorized user.

7. The Primary authorized user must configure a secure folder on their component network drive for installation of the database. This database must only be accessible by the CISS authorized users for the designated FISMA System Family. Contact the CMS_IT_Service_Desk to set us this folder.

ATTACHMENT C: INTERNAL JUSTIFICATION FOR CLOSURE INSTRUCTIONS AND TEMPLATE

A. INSTRUCTIONS

These are the instructions for identifying and managing findings that are infeasible to close using normal procedures. Typically, this process is initiated during the Corrective Action Plan (CAP) review, which follows the issuance of a formal deliverable, such as a Security Test and Evaluation Report, a SAS-70 report, or a Chief Financial Officer's (CFO) Report. At that time, both the subject of the review and the reviewer agree upon acceptable corrective actions that may be taken to remedy the finding and its associated weakness. If it is determined that the proposed CAP will not address all the issues contributing to the finding then this procedure can be initiated. In these rare cases, the following applies:

1. The request for finding closure must be initiated by the Business Owner.

2. Either the finding's original assigned risk level is low or compensating controls have been implemented to reduce the original assigned risk level to a low level. For the latter, the originator of the finding or an alternate authority designated by CMS must validate that compensating controls have been implemented and effectively mitigate the risk to a low level before the entity can submit a justification to close the finding.

3. The corrective action required to close the low risk finding must be either technically or financially unfeasible to accomplish.

4. The entity must submit to the CISO a formal risk acceptance form (see Attachment D), with the requested information within the form.

5. After review, the CISO decision will be returned using the approved format.

6. The entity's Information Security Risk Assessment (IS RA) must be updated to reflect the risk. Updating the IS RA must be included as a milestone in the CAP. It is not necessary for the entity to formally submit the IS RA until their next IS RA submission deadline.

7. Documentation, including both the updated IS RA and a copy of the decision notification, must be submitted via the CMS Integrated Security Suite (CISS).

8. The justification will be re-validated during subsequent CMS audits for relevancy to support on-going closure and potentially re-opened based on the following criteria:

    - A change in the technical environment enables the implementation of a technical control that was previously infeasible.
    - A change in the Security Requirements.
    - A change in the threat environment necessitates the implementation of additional security safeguards to maintain a constant and reasonable level of risk.

B. Notification Memo Template

This Notification Memo Template contains instructions, boiler plate text, and sample language. Enter data to the right of the colon symbol. (Example – Application Name: Security CBT). The shaded text enclosed with [brackets] must be deleted as each template must be customized to specifically address the component. Delete this paragraph prior to the submission of the Notification Memo.

This remainder of this page was intentionally left blank.

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Office of Information Services

DATE:

TO: **Business Owner:**
Title, Component Name:

FROM: CMS Chief Information Officer and
Director, Office of Information Services (OIS)

SUBECT: Justification for Closure of **Finding #:**

Based on the following explanation, **Component Name:** recommends that the above finding be closed.

Finding

Enter finding title and risk level. State the source of the finding, then copy finding text, in quotes.

Recommendation

Copy the recommendation text from the source text, in quotes.

Business Risk

***Describe the exposure to CMS business**. For example: Does this risk allow someone to modify sensitive data? Does it allow Information in Identifiable Form (IIF) to be seen? Can a Denial of Service be generated? Who can take advantage of this vulnerability?*

Risk Mitigation

***Describe what management, operational and/or technical controls are in place to limit exposure of this risk.** For example: Personnel screening, restricted physical access, firewalls, intrusion detection, segregated network, and so forth. **Describe any future plans to eliminate this risk**.*

Concurrence:

_____ _____

Julie Boughn Date
Chief Information Officer and Director
Office of Information Services

Non-Concurrence:

_____ _____

Julie Boughn Date
Chief Information Officer and Director
Office of Information Services

ATTACHMENT D: CMS INFORMATION SECURITY POLICY/STANDARD RISK ACCEPTANCE TEMPLATE

Component:	**System Name:**	**Subsystem:**	**Date:**
CMS System Security Level (FIPS-199 Categorization of information system): **High** ☐ **Moderate** ☐ **Low** ☐		**Requestor:**	**Phone Number:**
Overview of the Risk Acceptance Request (explain what is being requested)**:**			
Applicable Policy/Standard Affected (include brief description)**:**			
Finding from Audit: Not Applicable ☐ 1) Finding title and finding #: 2) Risk level: High ☐ Moderate ☐ Low ☐ 3) Source of finding: 4) Copy finding text in quotes: 5) Recommendation (copy recommendation text from source text in quotes): 6) Business Risk (describe the exposure to CMS business):			
Business Justification for the Risk Acceptance (What is the business impact to CMS of not accepting the request**):**			
Justification for Request (Explain why compliance with this policy/standard is not possible due to technical limitations, conflict with mission requirements, or other circumstances)**:**			
Risk Mitigation: **1)** Describe the compensating controls that will be implemented and, if applicable, the control number from NIST SP 800-53 to reduce the risk of otherwise complying with the policy/standard: **2)** Describe how the compensating controls in step 1 provide an equivalent security capability or level of protection for the information system:			

Additional Comments: Describe any additional information that may be needed or reference any attachments:

Endorsement of Risk Analysis Understanding and Acceptance

Concur ☐ **Non-Concur** ☐ **See Comments** ☐ _____

_____

Business Owner & Title
Date

Comments:_____
_____
_____
_____

Concur ☐ **Non-Concur** ☐ **See Comments** ☐ _____

_____

Information System Security Officer
Date

Comments:_____
_____
_____
_____

Concur ☐ **Non-Concur** ☐ **See Comments** ☐ _____

_____

Authorizing Official & Title
Date

Comments:_____
_____
_____
_____
_____
_____

Please note: If granted, this risk acceptance must be reviewed at least annually by the requesting component. Waivers must be renewed every three years or when significant changes which affect the system categorization, justification for noncompliance and/or compensating controls are made.

END OF DOCUMENT