CENTERS for MEDICARE & MEDICAID SERVICES

Information Security and Privacy Group

7500 Security Boulevard
Baltimore, Maryland 21244-1850

Risk Management Handbook
Volume III
Standard 6.2

Plan of Action and Milestones Process Guide

Final
Version 1.0
November 5, 2015

Table of Contents

1.0 Introduction

In accordance with the Federal Information Security Modernization Act (FISMA) of 2014[1], the Centers for Medicare and Medicaid Services (CMS) has implemented an Information Security and Privacy Program to protect the confidentiality, integrity, and availability of its information resources in compliance with applicable laws, regulations, and Executive Orders. The Risk Management Handbook (RMH) serves as a foundation on which the program is developed. It is a collection of documents that support processes to manage information security and privacy risks to the agency's operations. This Plan of Action and Milestones (POA&M) Process Guide is a part of the RMH[2], and is designed to effectively manage and mitigate organizational risk.

1.1 Purpose

The purpose of this guide is to provide information security personnel and stakeholders with guidance to aid in understanding, developing, maintaining, and reporting program- and system-level weaknesses and deficiencies to the Department of Health and Human Services (DHHS). It also provides the necessary requirements and protection for all POA&M information that is properly managed and entered into the CMS Federal Information Security Management Act Control Tracking System (CFACTS).

1.2 Background

The Office of Management and Budget (OMB) requires that all known weaknesses to be identified and tracked in a POA&M. OMB Memorandum M-04-25[3] states that a POA&M is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones to be passed in accomplishing the task, and scheduled dates for reaching each milestone. OMB requires stakeholders to regularly update the Chief Information Officer (CIO) on POA&M progress. The organization's CIO along with the Authorizing Official (AO) can monitor remediation efforts and provide the updates to OMB. All departments and agencies will prepare POA&Ms for all systems where an information security or privacy weakness has been found. Updates occur monthly or more frequently when the CIO directs. This task is accomplished through the use of the CFACTS tool.

This CMS POA&M guidance complies with the requirements prescribed by OMB, and includes information to account for the emphasis that has been placed on formalizing and prioritizing the weakness mitigation process.

[1] Federal Information Security Modernization Act of 2014 (FISMA), 44 USC 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899.

[2] The Risk Management Handbook (RMH), including the POA&M Process Guide, can be found on the IS Library using the following link: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

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

1.3 Scope

All CMS Business Owners (BO), System Developers and Maintainers (SDM), Information System Security Officers (ISSO), and any personnel tasked with completing POA&M activities should read this document and OMB guidelines to assist in implementing the CMS POA&M requirements. This guide outlines the requirements used to define, open, track (through the use of CFACTS), and remediate weaknesses. Users with POA&M responsibilities must understand the POA&M requirements process, the type of data involved, and the level of detail required to meet CMS and OMB requirements.

1.4 Applicability

This guide applies to all CMS FISMA information systems and programs where a security or privacy weakness has been identified. Within the context of this guide, "system" refers to any systems listed in the CMS FISMA system inventory.

1.5 Definition

The Plan of Action and Milestones (POA&M) is a remedial action plan (the process of accepting or resolving a risk) which helps the agency to identify and assess information system security and privacy weaknesses, set priorities, and monitor progress toward mitigating the weaknesses.[4] A POA&M helps with tracking and mitigating the following [NIST SP 800-32]:

- Risk Avoidance: Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. Risk avoidance is usually the most expensive of all risk mitigation options.

- Risk Transference: Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on their core competencies.

- Risk Acceptance: Risk acceptance does not reduce any effects however it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn't want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

- Risk Limitation: Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company's exposure by taking some action. It is a strategy employing a bit of risk acceptance along with a bit of risk avoidance or an average of both. An

[4] RMH_VI_10_Terms_Defs_Acronyms at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.

A POA&M is required for every system where an IT security or privacy weakness has been found. The findings stem from internal or external audits, reviews, and Continuous Diagnostic and Mitigation (CDM). Each finding identifies a weakness that must be resolved according to a POA&M.

A POA&M Corrective Action Plan (CAP) describes the measures that have been implemented or planned: (i) to correct any deficiencies noted during the assessment of the security and privacy controls; and (ii) to reduce or eliminate known vulnerabilities in the information system. It identifies: (i) the tasks needing to be accomplished; (ii) the resources required to accomplish the elements of the plan; (iii) any milestones with scheduled completion dates.

A POA&M must have at least one milestone. Once a milestone has been accepted and closed, the record must be retained for one year. Milestones should be S.M.A.R.T:

- *Specific* – target a specific area for improvement.
- *Measurable* – quantify or at least suggest an indicator of progress.
- *Assignable* – specify who will do it.
- *Realistic* – state what results can realistically be achieved, given available resources.
- *Time-related* – specify when the result(s) can be achieved.

A POA&M can be used for the following reasons:

- Assist management in identifying and tracking the progress of corrective actions
- Assist agencies in closing their security and privacy performance gaps
- Assist the Office of Inspector General (OIG) in evaluating agency security and privacy performance
- Assist OMB with its oversight responsibilities and the budget formalization process
- Assist with Congressional oversight by providing pre-decisional budget information

2.0 Roles and Responsibilities

CMS understands the cornerstone for the development of a sound information security and privacy program is cooperation and collaboration among all stakeholders safeguarding CMS information and information systems. The overall responsibility for POA&Ms rests with the CIO, but others such as the AO have significant roles as well. By authority of the CIO, the Chief Information Security Officer (CISO) is assigned responsibility for implementing and managing the agency’s information security and privacy program and for ensuring compliance with FISMA, OMB, and other Federal requirements relevant to information security and privacy. The CISO further delegates certain duties and responsibilities related to the POA&M management process to key security and privacy stakeholders including the Business Owners, the System Developers and Maintainers, and the Information System Security Officers.

The primary responsibility for information security and privacy rests with the government and its associated contractors. Contractors and others working on behalf of CMS may assist in the performance of security and privacy functions. The CMS Information Systems Security and Privacy Policy provides full descriptions of roles directly responsible for information system security and privacy[5]. A more detailed explanation of the roles and responsibilities related to POA&M management can be found in Appendix 3 of this guide.

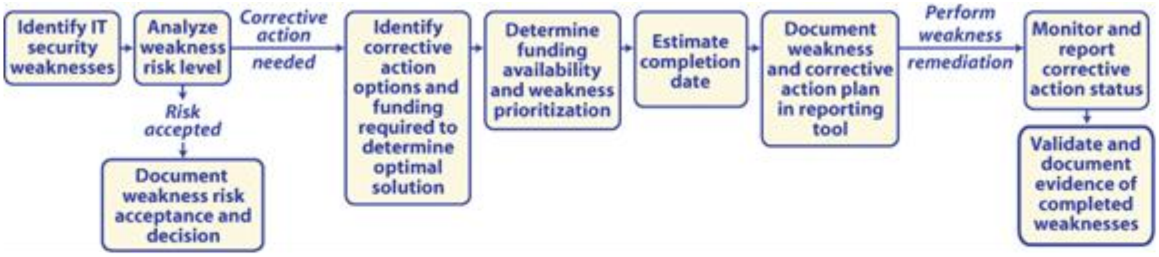
3.0 POA&M Overview

The POA&M process is a methodical approach to overseeing the resolution of weaknesses and reducing the risk to CMS Systems and Data. This process begins when a weakness or finding is identified, then the Business Owner and the AO are responsible for mitigating the risk.

The first steps in creating the POA&M are to develop a CAP, evaluate the financial costs for remediation, and provide a scheduled completion date. The plan is submitted to the Cyber Risk Advisor (CRA) for review. Once approved, the Business Owner executes the plan and provides monthly updates into CFACTS to document the mitigation efforts. The steps to the POA&M process are outlined below and will be described in greater detail throughout the remainder of this guide:

1. Identify IT Security and Privacy Weakness
2. Develop a Corrective Action Plan
3. Determine Funding Availability
4. Prioritize the Weakness
5. Assign a Scheduled Completion Date
6. Document the Corrective Action Plan
7. Manage to Completion
8. Validate Weakness Completion
9. Accept the Risk When Applicable

Figure 1 – The Weakness Remediation Process


Identify IT security weaknesses
Analyze weakness risk level
Corrective action needed
Risk accepted
Document weakness risk acceptance and decision
Identify corrective action options and funding required to determine optimal solution
Determine funding availability and weakness prioritization
Estimate completion date
Document weakness and corrective action plan in reporting tool
Perform weakness remediation
Monitor and report corrective action status
Validate and document evidence of completed weaknesses

3.1 Identify IT Security and Privacy Weaknesses

In POA&M terminology, the term "weakness" represents any information security or privacy vulnerability that could be exploited by a threat source resulting in the compromise of the confidentiality, integrity, or availability of an information system. All weaknesses that represent risk to the security or

[5] The CMS Policy for Information Security and Privacy (as amended) can be found on the CMS IS Library: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

privacy of a system must be corrected and the required mitigation efforts are captured in the POA&M. A weakness arises from a specific management, operational, or technical control deficiency and is entered individually on a system-specific POA&M.

3.1.1 Weakness Source

Weaknesses may originate from many sources and can be identified proactively or reactively. Proactive weakness determination occurs when regular 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. Weaknesses are documented by the source that identified them. At CMS, a weakness can be identified from any of a number of sources including, but not limited to:

- HHS Office of Inspector General (OIG) Audits
- Government Accountability Office (GAO) Audits
- Chief Financial Officer (CFO) Reviews
- OMB A-123 Internal Control Reviews
- Annual Assessments
- FISMA Audits
- Security Control Assessments
- Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) Section 912 Audits
- Internal Revenue Service (IRS) Safeguard Reviews
- Department of Homeland Security (DHS) Risk Vulnerability Assessments (RVA)
- DHS Cyber Hygiene
- Penetration Testing
- Vulnerability Scanning

The primary CMS owner, sponsor, or liaison for any assessment or audit is responsible for ensuring that any information security related findings are appropriately and completely documented in the CMS CAAT template, and that the completed template is provided to ISPG for upload into the CMS POA&M repository. Separate templates must be completed for each CMS IT program or FISMA system to which findings apply. The template must include a positive or negative test result for any control included within the scope of the assessment or audit. In essence, the CMS group which most directly scopes and/or interfaces with the assessor or auditor is responsible for ensuring the creation and submission of a complete CAAT template.

For example, in the case of a security control assessment, the independent third party assessor is employed by the CMS FISMA system business owner to conduct an assessment of their FISMA system. The business owner is responsible for ensuring that a complete CAAT template is created as part of the assessment. Typically the assigned ISSO will have been delegated day to day responsibility for the assessment and creation of the CAAT template. The assessment and creation of the CAAT template can be included in the reporting requirements for the third party assessor.

In cases where an area of CMS has authority to conduct audits of other business components within CMS, the auditing component or sponsor will ensure that the CAAT template is completed and provided to ISPG.

3.1.2 Determine the Root Cause

Root Cause Analysis (RCA) is an important and effective methodology used to correct an information security or privacy weakness by eliminating the underlying cause. Various factors are reviewed for an identified weakness. Inadequacies in one or more of the factors could be the root cause(s). Appendix 5 provides additional guidance and steps to follow when performing an RCA.

3.1.3 Weakness Severity Level

The severity level is based on the risk the weakness poses to the agency's overall security and privacy posture. There are three levels of severity as defined by OMB: significant deficiency, reportable condition, and weakness. An explanation of each severity level is provided in the following table:

Table 1 – Weakness Severity Levels

Weakness Severity Levels	
Significant Deficiency	A weakness is considered a *significant deficiency* if it drastically restricts the capability of the agency to carry out its mission or if it compromises the security or privacy of its information, information systems, personnel, or other resources, operations, or assets. In this case, senior management must be notified and immediate or near-immediate corrective action must be taken.
Reportable Condition	A *reportable condition* is a weakness that affects the efficiency and effectiveness of agency operations. Due to its lower associated risk, corrective actions for a reportable condition may be scheduled over a longer period of time. The control auditor or assessor will make the determination that a weakness is a reportable condition.
Weakness	All other weaknesses that do not rise to the level of a significant deficiency or reportable condition must be categorized as a *weakness* and mitigated in a timely manner and efficiently, as resources permit.

The weakness severity level can be obtained from the source or the audit report. Most findings will generally be categorized as a "weakness". However, in the event that a weakness is designated as a "significant deficiency", then contact the CISO mailbox (ciso@cms.hhs.gov) for further guidance.

3.1.4 Weakness Risk Level

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, "Risk Management Guide for Information Technology Systems," defines ***risk*** as, "the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence." It is a function of the likelihood that a threat-source could exploit a vulnerability and cause an adverse impact on the organization. Each identified weakness—unless there is not a threat—poses some level of risk to the system and the mission it supports.

NIST SP 800-30 provides a foundation for the development of an effective risk management program. It contains both the definitions and the practical guidance necessary for assessing and mitigating identified risks to IT systems. Risk level is dependent on multiple factors, such as Federal Information Processing Standard (FIPS) 199 category, operating environment, compensating controls, nature of the vulnerability, and impact if a system is compromised. If no risk level has been assigned by the assessor, the process described in NIST SP 800-30 may be used to help determine the proper risk level of a weakness. Table 2 shows the risk scale used at CMS:

Table 2 – Risk Scale

Risk Level	Risk Description and Necessary Management Action
High	A high risk indicates that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	A moderate risk indicates that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	A low risk indicates that threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

3.1.4.1 Common Controls Risk and Monitoring Frequency

Weaknesses or deficiencies in common controls have the potential to adversely affect large portions of the organization and require significant attention and more frequent monitoring. For example, one deficiency in the parent system affects all systems relying on that common control.

Monitoring frequency must be considered when determining whether a control weakness should be remediated as high, moderate, or low risk. Not all weaknesses require the same level of monitoring. In general, security and privacy controls implemented on systems that are categorized as high-impact are monitored more frequently than controls implemented on moderate-impact systems. In turn, controls implemented on a moderate-impact system must be monitored more frequently than controls implemented on low-impact systems. For example, technical controls**,** such as the Configuration Management (CM) family of controls, must be urgently remediated. Unanalyzed or unauthorized changes in the system configuration often render the system vulnerable to exploits and may require frequent assessment and monitoring.

3.2 Develop a Corrective Action Plan

After weaknesses have been identified and the root cause has been determined, a CAP or remediation strategy must be developed. The strategy should be a collaborative internal control effort with stakeholders including the CISO, Business Owners, System Developers and Maintainers, ISSOs, and others as needed. The stakeholders ensure that the remediation strategy is created, executed, and monitored. Depending on the risk level of the weakness, reasonable timeframes are granted for remediation: 90 days for a High-level risk, 180 days for a Moderate-level risk, and 365 days for a Low- or undefined-level risk.

3.3 Determine Funding Availability

OMB requires that each POA&M be tied to the planning agency's budget submission. The agency is required to identify the costs of providing IT security and privacy as part of the investment life cycle and to support infrastructure-related investments under FISMA. This integration produces tangible benefits by promoting enterprise security and privacy architecture and by supporting business operations. Funding requests and justifications are submitted to OMB using Exhibit 300 or 53[6] to develop and maintain the system.

Determining funding requirements and availability is the means by which IT security and privacy and capital planning and investment (CPIC) intersect within the POA&M process. The system's unique investment identifier (UII) provides the link to CMS' budget and ensures that the system's security and privacy weaknesses are funded. This identifier remains within the system throughout the system development lifecycle.

The weakness mitigation process requires resources; the type and amount of which will vary. Estimating the resources required should be done carefully. In estimating the resources required, there is no equation or formula that applies to every circumstance. However, there are some common factors that can be considered when making a funding determination, including:

- Evaluating the complexity of the CAP
- Evaluating the parties required to execute the CAP
- Determining the purchasing requirements
- Analyzing the risk and severity level of the weakness

The estimate of resources required must be based on the total resources needed to fulfill all the milestones[7] necessary for weakness correction. Appendix 7 provides a matrix to aid in the planning process of the POA&M. It provides estimates to address a range of data to ascertain the minimum resources reasonable for developing POA&Ms.

The type of funding (new, existing, or reallocated) should be noted in addition to the dollar amount and/or man hours. If new funding is required, the existing capital planning process should be relied upon to request and receive the necessary funds. If existing government personnel are assigned to correct the

[6] Office of Management and Budget. *OMB Circular A-11. Preparation, Execution, and Submission of the Budget.* July 2014.

[7] A POA&M must have at least one milestone.

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).

3.4 Prioritize the Weakness

CMS may assign priority of a weakness based on the risk level. FISMA guidance requires CMS to prioritize POA&M weaknesses to ensure the most critical security and privacy 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 stakeholders 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 is key to effective prioritization. Documented rank-ordering criteria enable the stakeholders 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:

Table 3 – Weakness Prioritization

Prioritization Factor	Description
Risk Level/Severity	Prioritization must take into account: • Sensitivity and criticality of information on the system. • The estimated likelihood of the weakness occurring and/or being exploited. • The cost of a potential occurrence/exploitation in terms of dollars, man-hours, and/or reputation.
Breadth	Is the weakness a systemic issue or is it an isolated event? Systemic issues represent much greater risk and should be viewed as a higher priority.
Source	What is the source of the weakness? An audit could expose a significant deficiency which demands greater attention.
Visibility	Has the weakness drawn a high level of external visibility? In some cases a lower level weakness is a higher priority due to visibility. There are times when senior management or outside organizations focus on a specific weakness that raises its priority beyond that of other, potentially higher risk, weaknesses.

Prioritization Factor	Description
Resources	What resources are required and available to aid in remediation or mitigation of the weakness? Some weaknesses can be quickly and easily resolved without much expenditure of time or money. In those cases, weaknesses may be addressed before those for which resourcing must be planned and budgeted.
Management Input	What input or recommendations have been obtained from management? Senior management and/or authorizing officials should have input into prioritizing weaknesses.
Analysis	The weakness must be analyzed to determine if there are any other processes or system relationships that it may affect. Does the weakness fall within the system boundary? Or perhaps is it a potential program weakness?
Other Weaknesses	Are there other weaknesses that overlap with the one in question? A combination of minor weaknesses may highlight a more serious problem.

3.5 Assign Scheduled Completion Dates

The scheduled date of completion for each weakness will be 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. The scheduled completion date will automatically be set by the CFACTS tool, according to the level of risk posed by the weakness: 90 days for a High-level risk, 180 days for a Moderate-level risk, and 365 days for a Low- or undefined-level risk.

The scheduled completion date will include the month, day, and year. The date will not exceed one year and may not be changed. Progress toward completion is tracked through milestones. If the time to correct the weakness extends beyond the original scheduled completion date, the status of the weakness will change to “delayed”, and reasons for the delay must be noted. A new scheduled completion date and reasons for the change must be annotated.

3.6 Document the Corrective Action Plan

OMB provides a standard, consistent POA&M format which is utilized at CMS. This structure improves the stakeholders’ ability to easily locate information and organize details for analysis. The CAP format includes a location for the identified program weakness, any associated milestones and necessary resources required. Once the CAP is documented, the plan must be entered into CFACTS in the form of a series of milestone records. The status of the POA&M will automatically be moved from “draft” to “ongoing” 30 days after the weakness creation date.

The milestones in the CAP must provide specific, action-oriented descriptions of the steps that the stakeholder will take to mitigate the weakness. The number of milestones articulated per weakness must 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 estimate completion date. Appendix 4 of this document provides samples of compliant and non-compliant milestones for use in documenting the CAP.

3.7 Manage to Completion

POA&M data must be monitored on a continuing basis and updated as events occur. CMS requires that all information in the POA&M be updated at least monthly and be accurate on the first day of each month for tracking and reporting purposes. As part of the review process, the ISSO will:

- Validate that the weakness is properly identified and prioritized
- Ensure that appropriate resources have been made available to resolve the weakness
- Ensure that the schedule for resolving the weakness is both appropriate and achievable

3.7.1 Weakness Status

A weakness status must 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 part of an ongoing monitoring process. Detailed descriptions of various statuses are summarized in the following table:

Table 4 - Status Descriptions

Status	Description
Draft	Indicates that a weakness requires review and approval prior to “official” entry in the POA&M. Types of review that may take place while a weakness is in draft status would be: reviewing to determine if the weakness already exists and would be a duplicate; reviewing to determine if the organization will accept the risk, or apply for a waiver; etc. After 30 calendar days, the POA&M status will be automatically changed to Ongoing/Open, and a scheduled completion date commensurate with the weakness risk level will be automatically assigned to it.
Ongoing	Assigned when a weakness is in the process of being mitigated and has not yet exceeded the original scheduled completion date.
Completed	Assigned when all corrective actions have been completed or closed for a weakness and the weakness has been verified as successfully mitigated. Documentation is required to demonstrate the weakness has been adequately resolved. When assigning the status of ‘Completed’, the date of completion must also be included.

Status	Description
Pending Verification	Indicates that all milestones/corrective actions have been completed but require review and sign-off to ensure effective resolution.
Delayed	Assigned when a weakness continues to be mitigated after the original scheduled completion date has passed. When the status changes to 'Delayed,' an explanation must be provided in the milestone as to why the delay is occurring, as well as the revised completion date.
Risk Accepted	Indicates that the weakness risk has been accepted by the Business Owner. When assigning this status, an acceptance of the risk must be certified by the Authorizing Official and documented accordingly. The weakness and corresponding risk must be monitored periodically, **but no less than annually**, to ensure the associated risk remains at an acceptable level.
Audit Approved	Indicates that a Completed POA&M has been audited by a member of the CISO's office or an independent third party.
Audit Rejected	Indicates that a Completed POA&M has been rejected by a member of the CISO's office or an independent third party. The individual responsible for the POA&M will be required to reconcile any noted discrepancy identified by auditor.

3.8 Verify Weakness Completion

OMB's FISMA reporting guidance recommends that weaknesses should be considered "Completed" only when fully resolved. The ISSO will provide evidence that the weakness has been resolved. Once complete, the ISSO will mark the POA&M closed in CFACTS. The CRA will review certain POA&M weaknesses, based upon a risk determination, and the evidence provided to ensure that the weakness has been adequately addressed and corrected.

Evidence may take many forms including, but not limited to: control test results, a policy or procedure document, a screenshot of a patch applied, or other new system documentation. The type and extent of evidence submitted must be commensurate with the sensitivity and criticality of the system and weakness in question. The artifacts are stored in CFACTS and retained for at least one year with the completed POA&M as well as under a Continuous Diagnostic and Mitigation (CDM) record.

3.9 Transfer Weaknesses

Weaknesses may only be removed due to transfer to another FISMA system POA&M, or retirement after 12 months with documentation within the POA&M. The transfer of POA&M weaknesses from one FISMA system to another must be clearly traceable and justified. The transfer must be accepted by the recipient system.

3.10 Completed Weaknesses

OMB M-04-25 advises that weaknesses that have been mitigated for over a year should no longer be reported to the department.

3.11 Accept the Risk When Applicable

A POA&M is a plan to resolve unacceptable risks. In rare cases, the Business Owner can present a case for accepting the risk to the Authorizing Official or CIO[8], who may make the decision to accept the risk at their discretion.

4.0 Reports

Reporting is a critical component of POA&M management, and CMS reports its remediation efforts on a monthly basis. The information in the POA&M must be maintained continuously to communicate overall progress.

OMB typically requires reporting on a quarterly or annual basis. Quarterly reports are usually focused on a specific area of interest. The reports are prepared by the CISO Office and provide the required information to DHHS on a quarterly basis for verification and analysis. DHHS compiles the information and sends a consolidated report to OMB.

5.0 CFACTS

Stakeholders must use CFACTS to identify, track, and manage all IT system weaknesses and associated POA&Ms to closure for CMS information systems. CFACTS is available at https://cfacts.cms.local. Users who need access to CFACTS may request an account and appropriate privileges through the Enterprise User Administration (EUA). The job code is CFACTS_User_P. Once the job code is assigned, the user must email the CISO mailbox at ciso@cms.hhs.gov to notify the CISO of the user's role (ISSO, SDM or BO).

The CFACTS User Manual provides detailed instructions for processing POA&M actions in the CFACTS tracking system. The User Manual can be accessed on the CFACTS welcome page under the CFACTS Documents section. In the manual, the user can find step by step procedures for creating, modifying, tracking and reporting POA&Ms. It explains the various sections in a POA&M record, and the various data fields that must be captured to meet OMB and CMS requirements. Support for CFACTS and offline copies of the User Manual are available by emailing the CISO mailbox.

[8] The CMS Information Security Risk Acceptance Template can be found on the Information Security and Privacy Library using the following link: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. This link will direct you to the appropriate forms required to document the waiver. The waiver form can also be completed in the CFACTS application.

Appendix 1 – Acronyms

A complete list of the Security and Privacy Program's standard acronym definitions can be found in the CMS RMH Vol 1 Chapter 10, CMS Risk Management Terms, Definitions, and Acronyms.

Acronym	Meaning
A&A	Assessment and Authorization
AO	Authorizing Official
AP	Authorization Package
ARS	Acceptable Risk Safeguards
ATO	Authorization to Operate
BO	Business Owner
CAAT	CMS Assessment and Audit Tracking
CAP	Corrective Action Plan
CCR	Critical Control Review
CFACTS	CMS Federal Information Security Management Act Control Tracking System
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
CMSR	CMS Minimum Security Requirements
CPIC	Capital Planning and Investment Control
CRA	Cyber Risk Advisor
DCISO	Deputy CISO
DHHS	Department of Health and Human Services
ECD	Estimated Completion Date
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTI	Federal Tax Information
GAO	Government Accountability Office
GSS	General Support System
ISPG	Information Security and Privacy Group
ISSO	Information Systems Security Officer
IV&V	Independent Verification and Validation
MA	Major Application
NIST	National Institute of Standards and Technology
OEI	Office of Enterprise Information

Acronym	Meaning
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OpDiv	Operating Division
OTS	Office of Technology Solutions
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
RCA	Root Cause Analysis
RMF	Risk Management Framework
RMH	Risk Management Handbook
RVA	Risk Vulnerability Assessment
SAR	Security Assessment Report
SCA	Security Control Assessment
SDM	System Developer and Maintainer
SOP	Senior Official for Privacy
SSP	System Security Plan
TRA	Technical Reference Architecture
TRB	Technical Review Board
UII	Unique Investment Identifier

Appendix 2 – Glossary

A complete list of the Security and Privacy Program's standard acronym definitions can be found in the CMS RMH Vol 1 Chapter 10, CMS Risk Management Terms, Definitions, and Acronyms.

Term	Definition
A-123 Reviews	Management's Responsibility for Internal Control. Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.
Annual Assessment	The process of validating the effective implementation of security and privacy controls in the information system and its environment of operation within every three hundred sixty-five (365) days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.
Audit	An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Capital Planning and Investment Control	A decision-making process for ensuring that investments integrate strategic planning, budgeting, procurement, and the management of or in support of Agency missions and business needs. [OMB Circular No. A-11]. The term comes from the Clinger-Cohen Act of 1996; while originally focused on IT, it now applies also to non-IT investments.
Common Control	A security or privacy control that is inherited by one or more organizational information systems. *See Security Control Inheritance.*
Completed	A status assigned when all corrective actions have been completed or closed for a weakness and the weakness has been verified as successfully mitigated. Documentation is required to demonstrate the weakness has been adequately resolved. When assigning the status of 'Completed', the date of completion must also be included.
Completion Date	The action date when all weaknesses have been fully resolved and the corrective action plan has been tested.
Control Activities	The policies and procedures that help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities, whether automated or manual, help achieve control objectives and are applied at various organizational and functional levels.

Term	Definition
Control Deficiency	A deficiency that exists when the design or operation of a control does not allow management or employees to, in the normal course of performing their assigned functions, prevent or detect breaches of confidentiality, integrity, or availability on a timely basis. (See also design deficiency or operations deficiency)
Corrective Action Plan (CAP)	The plan management formulates to document the procedures and milestones identified to correct control deficiencies.
Criteria	A context for evaluating evidence and understanding the findings, conclusions, and recommendations included in the report. Criteria represent the laws, regulations, contracts, grant agreements, standards, specific requirements, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation.
Delayed	A status assigned when a weakness continues to be mitigated after the original scheduled completion date has passed. When assigning the status of 'Delayed,' an explanation must be provided in the milestone as to why the delay is occurring, as well as the revised completion date.
Design Deficiency	A deficiency that exists when a control necessary to meet the control objective is missing or an existing control is not properly designed, so that even if the control operates as designed the control objective is not always met.
Draft	A status that indicates that a weakness requires review and approval prior to "official" entry in the POA&M. Types of review that may take place while a weakness is in draft status would be: reviewing to determine if the weakness already exists and would be a duplicate; reviewing to determine if the organization will accept the risk, or apply for a waiver; etc.
Evidence	Any information used by the auditor, tester, or evaluator, to determine whether the information being audited, evaluated, or assessed is stated in accordance with the established criteria.
Exhibit 300 Business Case	Exhibit 300 business cases are also referred to as capital asset plans. They are required by OMB Circular A-11 and provide budget justification and reporting requirements for investments. They provide agencies with the format to report on the budgeting, acquisition, and management of federal capital assets.
Exhibit 53	Also referred to as agency IT investment portfolios. They are required by OMB Circular A-11 and provide summary budget information for all agency major and non-major IT investments.
FISMA Audit	A FISMA assessment designed to determine areas of compliance and areas requiring remediation to become FISMA compliant.
Federal Information Security Modernization Act (FISMA)	Requires agencies to integrate information technology (IT) security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the OMB. [NIST SP 800-65]

Term	Definition
Findings	Conclusions based on an evaluation of sufficient, appropriate evidence against criteria.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and /or information systems.
Information System Security Officer (ISSO)	Individual with assigned responsibility for maintaining the appropriate operational security and privacy posture for an information system or program.
Initial Audit findings	Any type of audit conducted on a financial system or a non-financial system.
Internal Control	An integral component of an organization's management systems that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, or compliance with applicable laws and regulations.
Management Controls	The security or privacy controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security and privacy.
Material Weakness	Material weaknesses for FMFIA overall include reportable conditions in which the Secretary or Component Head determines to be significant enough to report outside of the Department. Material weakness in internal control over financial reporting is a reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.
Metrics	Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
Non-conformance	Instances in which financial management systems do not substantially conform to financial systems requirements. Financial management systems include both financial and financially-related (or mixed) systems.
Ongoing	A status assigned when a weakness is in the process of being mitigated and has not yet exceeded the original scheduled completion date.
Operational Controls	The security or privacy controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Operations Deficiency	A deficiency that exists when a properly designed control does not operate as designed or when the person performing the control is not qualified or properly skilled to perform the control effectively.

Term	Definition
Pending Verification	A status that indicates that all milestones/corrective actions have been completed but require review and sign-off to ensure effective resolution.
Plan of Action and Milestones (POA&M)	A FISMA mandated corrective action plan to identify and resolve information security and privacy weaknesses. A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Program	An organized set of activities directed toward a goal or particular set of goals or objectives for which the program is accountable; a distinct set of activities and strategies organized toward achieving a specific purpose. A program is a representation of what is delivered to the public. Programs usually operate for indefinite or continuous periods, but may consist of several projects or initiatives.
Reportable Condition	Reportable conditions overall include a control deficiency, or combination of control deficiencies, that in management's judgment, must be communicated because they represent significant weaknesses in the design or operation of an internal control that could adversely affect the organization's ability to meet its internal control objectives.
Resilience	The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. *[NIST SP 800-39, Adapted]*
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security and privacy risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Accepted	A status assigned when the weakness risk has been accepted. When assigning this status, an acceptance of the risk must be certified by the appropriate Authorizing Official and documented accordingly. The weakness and corresponding risk must be monitored periodically to ensure the associated risk remains at an acceptable level.

Term	Definition
Safeguards	Protective measures prescribed to meet the security and privacy requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security and privacy features, management constraints, personnel security, and security of physical structures, areas, and devices; synonymous with security and privacy controls and countermeasures.
Scheduled or Estimated Completion Date	A realistic estimate of the amount of time it will take to complete all associated milestones for a POA&M.
Security Control Assessment (SCA)	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST SP 800-37]
Security Control Inheritance	A situation in which an information system or application receives protection from security and privacy controls (or portions of security and privacy controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. *See Common Control.*
Significant Deficiency	A weakness in an agency's overall information systems security and privacy program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security or privacy of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.
Technical Controls	Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [FIPS 200]
Threat	Any potential danger to information or systems. A potential threat event, if realized, would cause an undesirable impact. The undesirable impact can come in many forms, but often results in a financial loss. A threat agent could be an intruder accessing the network through a port on the firewall, a process of accessing data in a way that violates that security or privacy policy, a tornado wiping out a facility, or an employee making an unintentional mistake that could expose confidential information or destroy a file's integrity.
Vulnerability	The absence or weakness of a safeguard that could be exploited; the absence or weakness of cumulative controls protecting a particular asset. Vulnerability is a software, hardware, or procedure weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment.

Term	Definition
Waiver	A status provided when the weakness risk has been accepted and justification has been appropriately documented. Justification of non-compliance must follow the agency's waiver policy and be documented accordingly.
Weakness	The absence of adequate controls.

Appendix 3 – Roles and Responsibilities

Role	Responsibilities
Chief Information Officer (CIO)	Communicates weaknesses and risks to CMS Administrator and senior officials, and escalates POA&M information as appropriate Reports quarterly to the DHHS CIO on the effectiveness of the IT security and privacy program, including the progress of the agency's remediation efforts Establishes standards for system security and privacy risk, more stringent than the DHHS standard Implements the system security and privacy risk management and monitoring program and submit requests for higher-risk deviations from the enterprise standard Delegates the responsibility for the oversight and management of POA&Ms to the CISO Serves as the Authorizing Official Oversees and monitors progress of the POA&M implementation and remediation efforts Ensures that corrective action plans for all systems are developed, implemented, and managed Approves all waivers and exceptions to CMS policy
Chief Information Security Officer (CISO)	Leads the agency's IT security and privacy programs and promotes proper IT security and privacy practices Develops information security and privacy policy, establishes the standards for system security risk, oversees risk management and monitoring Oversees and maintains the CMS POA&M process Ensures the POA&M process prioritizes corrective actions for information security and privacy weaknesses

Role	Responsibilities
	Ensures that information security and privacy weaknesses are addressed in a timely manner Escalates critical weaknesses and risks to CIO in a timely manner Conducts independent reviews of POA&M quality Ensures all POA&M data reflects the current state of security and privacy weaknesses across the agency and meets related Federal and Departmental reporting requirements Ensures timely submission of POA&M data to HHS CISO Ensures available funding for weakness mitigation Allocates proper resources to permit identification and remediation of the Information Security and Privacy Group (ISPG) system weaknesses Allocates proper resources to support Department-wide POA&M process implementation and reporting mechanisms
Cyber Risk Advisor	Works with Business Owners and ISSOs to build and implement a comprehensive POA&M process Monitors progress of the POA&M implementation efforts Audit a selection of POA&Ms based on risk criteria Conducts quarterly reviews of the consistency and accuracy of the POA&M data Ensures that CFACTS is used to develop, track, and manage the remediation of IT system and program weaknesses

Role	Responsibilities
Business Owners (BO)	Responsible for the successful operation and security and privacy of the information systems and programs within the program area Appoints an ISSO for each information system managed Works with ISSOs or other designated security and privacy personnel to develop, implement, and manage system-level CAP for weaknesses in all systems that support their operations and assets Ensures development of a POA&M to address weaknesses and deficiencies in the information system Aids in the prioritization of weaknesses based on severity and/or criticality of the system Ensures that information security and privacy requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance Updates CMS management regularly on the progress of weakness remediation efforts Escalates issues related to critical weaknesses in a timely manner Ensures training and oversight for personnel with significant security responsibilities Must be a federal employee at the Group Director level or above
System Developer and Maintainer (SDM)	Develops, implements, and manages system level corrective action plans that involve modifications and enhancements Provides regular updates on the progress of remediation for weaknesses Must be a federal employee at the Division Director level or above
Information System Security Officers (ISSO)	Serves as the appointed contact person, as delegated by the business owner, for all security and privacy matters related to the information system (An ISSO can manage more than one system and an ISSO can have alternates)

Role	Responsibilities
	Ensures the implementation and maintenance of security and privacy controls in accordance with the System Security Plan (SSP) and CMS policies Works with Business Owners and System Developers/Maintainers to develop, implement, and manage CAPs for all information systems they own and/or operate Aids in the prioritization of weaknesses based on severity and/or criticality of the system Ensures POA&Ms are entered into CFACTS for all IT security and privacy weaknesses Ensures that the POA&M contains appropriate details, as required by OMB and DHHS Conducts follow-up to verify a corrective action's status Ensures remediation and closure of POA&Ms in accordance with CMS policy Updates ISPG on a regular basis (at least monthly) regarding the progress of the mitigation activities of each weakness

Appendix 4 – Sample Milestone Descriptions

This Appendix provides examples of both fully-compliant, as well as non-compliant, milestones as outlined by OMB and CMS guidance.

Compliant Sample Milestones

Below are sample milestones that properly capture the actions that are needed to resolve the weakness. They include steps for planning, testing, implementing and documenting the proposed solution. In some cases, the root cause is also clearly being addressed. These are examples of how milestones should be written.

Sample 1

- Investigate options for verifying supervisor approval of Form 20-24.
- Select most suitable option and update procedures.
- Implement ongoing process for re-certifying system users.
- Test effectiveness of new process by cross checking form 20-24 against active user list.

Sample 2

- Develop SOPs to define and assign specific roles and responsibilities for managing accounts on the system.
- Define a process to disable accounts after a person has left CMS.
- Hand over control of the system from Engineering to Operations Team. Provide formal document or email with handoff signature.
- Define password expiration and verify that the setting is in place for the system. Accounts should lock out or expire after a defined period of inactivity.
- Assure that CMS password guidelines are being followed for complexity on this system. Provide a screenshot of this setting.

Sample 3

- Submit a system change request to the technical review committee to set failed login threshold.
- Set login threshold and analyze any negative effects that may occur from new configuration.
- Test logon threshold within TDL.
- Deploy threshold to production environment.

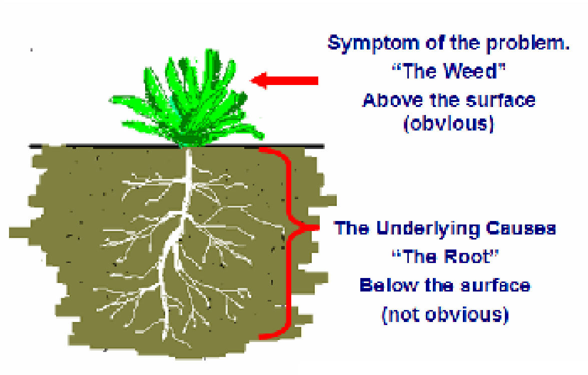
Non-Compliant Sample Milestones

The following table provides a sample list of non-compliant milestones along with the corresponding rationale. Defining milestones appropriately is the most critical element of the POA&M process. Without clearly defined milestones, it is difficult to determine the actions that need to be taken and the responsible party for completing the task. It is also difficult to determine when the weakness has been resolved.

Milestone	Rationale for Failure
Mitigate all high level weaknesses	The milestone does not provide a plan for mitigating any specific weakness.
Take the required preparatory steps to resolve all issues found at this site	The milestone does not provide a plan for mitigating the weakness.
Create plan of action to mitigate the finding or provide a Risk Acceptance letter	The POA&M ***is*** the plan to mitigate the finding. A POA&M to develop a POA&M is not sufficient.
Ensure the policy is followed	This was the only milestone and does not provide a plan for how to ensure the policy is followed.
Multifactor authenticators are required for Privileged Accounts	Restates the requirement. Does not provide a plan for resolving the issue. Appropriate milestones may include: Identify authenticators that satisfy the requirement Obtain/procure authenticators. Install required hardware/software. Test implementation of authenticators. Distribute authenticators to privileged account holders. Update SSP and other system documents.
We will apply the fix	The milestone does not provide a plan for mitigating any specific weakness.

Appendix 5 – Root Cause Analysis

Root Cause Analysis (RCA*)* is a structured systems analysis methodology whose purpose is to identify the underlying causes of problems, issues, or events. The goal of RCA is to resolve the problem by attempting to correct or eliminate the underlying causes. Correcting the underlying root cause may eliminate more than one seemingly unrelated symptom or address a prevalent issue across an entire organization.



Reasons for conducting a root cause analysis include:

- Identifying causes for weaknesses in order to strengthen issues which are hindering progress
- Reducing the likelihood of recurrence by focusing corrective actions on the cause versus the symptomatic conditions which are more frequently reported
- Assisting the CISO, Business Owners, and ISSOs with the assignment of risk and subsequent prioritization for remediation

When performing an RCA, always consider the policies, procedures, people, and resources in the investigation. Brainstorming with multiple people with varying backgrounds and expertise should be encouraged to develop the most robust solutions. At a minimum, the following steps are recommended when conducting an RCA:

- Understand the impact of the identified problem on business or mission needs. Try to first understand the context for the problem and the stakeholders. Do not start investigating possible solutions until the problem is defined from the people, process, and technology perspectives.
- Consider the known threats and vulnerabilities associated with the weakness and understand the risk and impact.
- Work with the CISO, Business Owners, and ISSOs to help prioritize the order in which the weaknesses should be addressed. For example, is it a significant deficiency or a reportable condition? Does it impact more than one system or site?
- Review the applicable policies and procedures to determine if the CMS guidance is being appropriately and consistently applied. Contact ISPG's Division of Security, Privacy Policy, and Governance if clarifications are needed.
- Identify the resources required to address the issue:

  - Staffing – Determine if the staff are aware of and understand the policies and procedures or if additional training is required.
  - Funding – Determine if current resources can address the weakness or if additional, long range funding will be required and requested.
  - Systems – Determine whether the hardware platform, operating system, and application software are adequate.

Common Root Causes

The following is a partial list of examples of root cause considerations:

- Policy and Procedures
  - Component policies have not implemented a recently required CMS update
  - NIST control procedure requirements are missing or the control design is inadequately documented to reflect the implementation requirement
- Processes
  - Standard Operating Procedures are not being followed, i.e. Emergency Fixes applied without record of change management approvals
  - Notification of critical security patches are not received by the staff and tracked for implementation
- People (Staff)
  - Poor or inconsistent communication between the Business Owner, ISSO, and System Developer and Maintainer
  - Assigned ISSO supporting higher priority collateral duties
  - Staff is not properly trained to perform functions
- Systems Technology
  - The hardware platform has reached end of life and is no longer being upgraded and only basic hardware maintenance activities are supported
  - The operating system does not include configuration management for hardening
  - Insecure services or default accounts are not removed
  - Security Log Files not turned on or being overwritten

Appendix 6 – POA&M Checklist

For an existing POA&M record use the following checklist to submit the POA&M for review.

S.No	Task	Required/Optional	Status (Check when completed)
1	Add Milestones (More than 1 milestone can be added)	Required	
2	Update Milestones – Changes to Milestone	Optional – When there is any changes to Milestone or for Milestone Status update on a monthly basis.	
3	Provide funding source, labor and cost estimate in Schedule vs. Actual section	Required	
4	Assign POA&M Owner in POA&M Submission section	Required	
5	Assign POA&M Reviewer in Review Section	Required (Recommended not to have the same person assigned as POA&M owner and reviewer for a given POA&M)	
6	When **complete** provide the Actual completion Date for each milestone.	Required	
7	Check if all milestones have been completed?	Required	
8	Upload Remediation related artifacts in Remediation Evidence section	Optional (Recommended to provide artifacts that can be considered as remediation evidence)	
9	Submit POA&M for review by changing the POA&M Status field in POA&M Submission section and selecting the priority for review in Review section	Required	
10	To complete the POA&M review the POA&M reviewer will select appropriate Review Status in Review Section	Required (By POA&M Reviewer)	

Appendix 7 – Resources Matrix

Control Number	Control Name	Minimum Resources
AC-1	Access Control Policy And Procedures	≥ $400
AC-2	Account Management	≥ $50
AC-3	Access Enforcement	≥ $50
AC-4	Information Flow Enforcement	≥ $200
AC-5	Separation of Duties	≥ $200
AC-6	Least Privilege	≥ $250
AC-7	Unsuccessful Login Attempts	≥ $50
AC-8	System Use Notification	≥ $50
AC-9	Previous Logon (Access) Notification	≥ $50
AC-10	Concurrent Session Control	≥ $50
AC-11	Session Lock	≥ $50
AC-12	Session Termination (Withdrawn)	≥ $50
AC-13	Supervision and Review—Access Control (Withdrawn)	≥ $400
AC-14	Actions Permitted Without Identification or Authentication	≥ $200
AC-15	Automated Marking (Withdrawn)	≥ $50
AC-16	Security Attributes	≥ $50
AC-17	Remote Access	≥ $2000
AC-18	Wireless Access	≥ $2000
AC-19	Access Control for Mobile Devices	≥ $4000
AC-20	Use of External Information Systems	≥ $400
AC-21	User-Based Collaboration and Information sharing	≥ $400
AC-22	Publicly Accessible Content	≥ $400
AT-1	Security Awareness and Training Policy and Procedures	≥ $400

Control Number	Control Name	Minimum Resources
AT-2	Security Awareness	≥ $2000
AT-3	Security Training	≥ $4000
AT-4	Security Training Records	≥ $4000
AT-5	Contacts with Security Groups and Associations	≥ $400
AU-1	Audit and Accountability Policy and Procedures	≥ $400
AU-2	Auditable Events	≥ $400
AU-3	Content of Audit Records	≥ $400
AU-4	Audit Storage Capacity	≥ $400
AU-5	Response to Audit Processing Failures	≥ $800
AU-6	Audit Review, Analysis, and Reporting	≥ $400
AU-7	Audit Reduction and Report Generation	≥ $1000
AU-8	Time Stamps	≥ $50
AU-9	Protection of Audit Information	≥ $50
AU-10	Non-Repudiation	≥ $50
AU-11	Audit Record Retention	≥ $400
AU-12	Audit Generation	≥ $100
AU-13	Monitoring for Information Disclosure	≥ $100
AU-14	Session Audit	≥ $100
CA-1	Security Assessment and Authorization Policies and Procedures	≥ $400
CA-2	Security Assessments	≥ $5000
CA-3	Information System Connections	≥ $2000
CA-4	Security Certification (Withdrawn)	≥ $92000
CA-5	Plan of Action and Milestones	≥ $1800
CA-6	Security Authorization	≥ $500

Control Number	Control Name	Minimum Resources
CA-7	Continuous Monitoring	≥ $100
CM-1	Configuration Management Policy and Procedures	≥ $400
CM-2	Baseline Configuration	≥ $4000
CM-3	Configuration Change Control	≥ $4000
CM-4	Security Impact Analysis	≥ $2400
CM-5	Access Restrictions for Change	≥ $50
CM-6	Configuration Settings	≥ $50
CM-7	Least Functionality	≥ $50
CM-8	Information System Component Inventory	≥ $400
CM-9	Configuration Management Plan	≥ $100
CP-1	Contingency Planning Policy and Procedures	≥ $400
CP-2	Contingency Plan	≥ $5200
CP-3	Contingency Training	≥ $2500
CP-4	Contingency Plan Testing and Exercises	≥ $10000
CP-5	Contingency Plan Update (Withdrawn)	≥ $1200
CP-6	Alternate Storage Sites	≥ $4000
CP-7	Alternate Processing Sites	≥ $4000
CP-8	Telecommunications Services	≥ $4000
CP-9	Information System Backup	≥ $200
CP-10	Information System Recovery and Reconstitution	≥ $400
IA-1	Identification and Authentication Policy and Procedures	≥ $400
IA-2	Identification and Authentication (Organizational Users)	≥ $50
IA-3	Device Identification and Authentication	≥ $50
IA-4	Identifier Management	≥ $400

Control Number	Control Name	Minimum Resources
IA-5	Authenticator Management	≥ $50
IA-6	Authenticator Feedback	≥ $400
IA-7	Cryptographic Module Authentication	≥ $100
IA-8	Identification and Authentication (Non-Organizational Users)	≥ $400
IR-1	Incident Response Policy and Procedures	≥ $400
IR-2	Incident Response Training	≥ $400
IR-3	Incident Response Testing and Exercises	≥ $1200
IR-4	Incident Handling	≥ $1200
IR-5	Incident Monitoring	≥ $400
IR-6	Incident Reporting	≥ $400
IR-7	Incident Response Assistance	≥ $100
IR-8	Incident Response Plan	≥ $400
MA-1	System Maintenance Policy and Procedures	≥ $400
MA-2	Controlled Maintenance	≥ $800
MA-3	Maintenance Tools	≥ $400
MA-4	Non-Local Maintenance	≥ $400
MA-5	Maintenance Personnel	≥ $50
MA-6	Timely Maintenance	≥ $2000
MP-1	Media Protection Policy and Procedures	≥ $400
MP-2	Media Access	≥ $400
MP-3	Media Marking	≥ $400
MP-4	Media Storage	≥ $400
MP-5	Media Transport	≥ $400
MP-6	Media Sanitization	≥ $400

Control Number	Control Name	Minimum Resources
PE-1	Physical and Environmental Protection Policy and Procedures	≥ $400
PE-2	Physical Access Authorizations	≥ $50
PE-3	Physical Access Control	≥ $50
PE-4	Access Control for Transmission Medium	≥ $50
PE-5	Access Control for Output Devices	≥ $50
PE-6	Monitoring Physical Access	≥ $800
PE-7	Visitor Control	≥ $400
PE-8	Access Records	≥ $400
PE-9	Power Equipment and Power Cabling	≥ $100
PE-10	Emergency Shutoff	≥ $50
PE-11	Emergency Power	≥ $50
PE-12	Emergency Lighting	≥ $50
PE-13	Fire Protection	≥ $50
PE-14	Temperature and Humidity Controls	≥ $50
PE-15	Water Damage Protection	≥ $50
PE-16	Delivery and Removal	≥ $400
PE-17	Alternate Work Site	≥ $50
PE-18	Location of Information System Components	≥ $1000
PE-19	Information Leakage	≥ $1000
PL-1	Security Planning Policy and Procedures	≥ $400
PL-2	System Security Plan	≥ $4000
PL-3	System Security Plan Update (withdrawn)	≥ $2000
PL-4	Rules of Behavior	≥ $400
PL-5	Privacy Impact Assessment	≥ $200

Control Number	Control Name	Minimum Resources
PL-6	Security-Related Activity Planning	≥ $50
PS-1	Personnel Security Policy and Procedures	≥ $400
PS-2	Position Categorization	≥ $50
PS-3	Personnel Screening	≥ $50
PS-4	Personnel Termination	≥ $50
PS-5	Personnel Transfer	≥ $50
PS-6	Access Agreements	≥ $50
PS-7	Third-Party Personnel Security	≥ $400
PS-8	Personnel Sanctions	≥ $50
RA-1	Risk Assessment Policy and Procedures	≥ $400
RA-2	Security Categorization	≥ $200
RA-3	Risk Assessment	≥ $4000
RA-4	Risk Assessment Update (Withdrawn)	≥ $2000
RA-5	Vulnerability Scanning	≥ $400
SA-1	System and Services Acquisition Policy and Procedures	≥ $400
SA-2	Allocation of Resources	≥ $400
SA-3	Life Cycle Support	≥ $400
SA-4	Acquisitions	≥ $400
SA-5	Information System Documentation	≥ $400
SA-6	Software Usage Restrictions	≥ $50
SA-7	User Installed Software	≥ $400
SA-8	Security Engineering Principles	≥ $400
SA-9	External Information System Services	≥ $400
SA-10	Developer Configuration Management	≥ $400

Control Number	Control Name	Minimum Resources
SA-11	Developer Security Testing	> $4000
SA-12	Supply Chain Protection	> $400
SA-13	Trustworthiness	> $400
SA-14	Critical Information System Components	> $400
SC-1	System and Communications Protection Policy and Procedures	> $400
SC-2	Application Partitioning	> $50
SC-3	Security Function Isolation	> $50
SC-4	Information in Shared Resources	> $50
SC-5	Denial of Service Protection	> $50
SC-6	Resource Priority	> $ 50
SC-7	Boundary Protection	> $50
SC-8	Transmission Integrity	> $100
SC-9	Transmission Confidentiality	> $100
SC-10	Network Disconnect	> $50
SC-11	Trusted Path	> $50
SC-12	Cryptographic Key Establishment And Management	> $50
SC-13	Use of Cryptography	> $50
SC-14	Public Access Protections	> $50
SC-15	Collaborative Computing Devices	> $50
SC-16	Transmission of Security Attributes	> $50
SC-17	Public Key Infrastructure Certificates	> $400
SC-18	Mobile Code	> $400
SC-19	Voice Over Internet Protocol	> $400
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	> $100

Control Number	Control Name	Minimum Resources
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	≥ $100
SC-22	Architecture and Provisioning for Name/Address Resolution Service	≥ $100
SC-23	Session Authenticity	≥ $100
SC-24	Fail in Known State	≥ $50
SC-25	Thin Nodes	≥ $50
SC-26	Honeypots	≥ $50
SC-27	Operating System-Independent Applications	≥ $50
SC-28	Protection of Information at Rest	≥ $50
SC-29	Heterogeneity	≥ $50
SC-30	Virtualization Techniques	≥ $50
SC-31	Covert Channel Analysis	≥ $50
SC-31	Information System Partitioning	≥ $50
SC-33	Transmission Preparation Integrity	≥ $50
SC-34	Non-Modifiable Executable Programs	≥ $50
SI-1	System and Information Integrity Policy and Procedures	≥ $400
SI-2	Flaw Remediation	≥ $50
SI-3	Malicious Code Protection	≥ $50
SI-4	Information System Monitoring	≥ $50
SI-5	Security Alerts, Advisories, and Directives	≥ $50
SI-6	Security Functionality Verification	≥ $50
SI-7	Software and Information Integrity	≥ $50
SI-8	Spam Protection	≥ $50
SI-9	Information Input Restrictions	≥ $50
SI-10	Information Input Validation	≥ $50

Control Number	Control Name	Minimum Resources
SI-11	Error Handling	> $50
SI-12	Information Output Handling and Retention	> $50
SI-13	Predictable Failure Prevention	> $50

Appendix 8 – References

Federal Laws

Federal Information Security Management Act of 2002 (FISMA), 44 USC 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899.

OMB Circulars

Office of Management and Budget. *OMB Circular A-11. Preparation, Execution, and Submission of the Budget.* July 2014.

Office of Management and Budget. *OMB Circular A-130. Management of Federal Information Resources.* November 2000.

OMB Memorandums

Office of Management and Budget. *OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act*. August 2004. Retrieved from http://www.whitehouse.gov/omb/memoranda/index.html.

Office of Management and Budget. *OMB Memorandum M-11-33, FY2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* September 2011. Retrieved from http://www.whitehouse.gov/omb/memoranda/index.html.

Agency Publications

Centers for Medicare and Medicaid Services, Enterprise Information Security Group. *Risk Management Handbook, Volume II, Procedure 6.2, POA&M Management, Version 1.01*, July 2012.

Centers for Medicare and Medicaid Services, Office of Information Services. *CMS Plan of Action and Milestones (POA&M) Guidelines, Version 1.0.* June 2007.

Department of Homeland Security. *DHS 4300A, Sensitive Systems Handbook, Attachment H, Process Guide for Plan of Action and Milestones, Version 9.1.* July 2012.

Department of Health and Human Services, Office of the Chief Information Security Officer. *HHS Plan of Action and Milestones Guide, Version 1.0.* March 2013.

Department of Health and Human Services, Office of the Chief Information Officer. *Standards for Plans of Action and Milestones Management.* November 2012.

NIST Federal Information Processing Standards (FIPS)

National Institute of Standards and Technology (NIST). *Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*. February 2004.

NIST Information Technology Security Special Publications (SP)

National Institute of Standards and Technology (NIST). *Special Publications (SP) 800 Series (e.g., NIST SP 800-53, Rev 3, Recommended Security Controls for Federal Information Systems and Organizations.* August 2009, updated May 2010. Retrieved from http://csrc.nist.gov/publications/nistpubs/index.html

APPROVED

\s\

Emery Csulak
CMS Chief Information Security Officer (CISO) and
Senior Official for Privacy (SOP)

This document will be reviewed periodically, but no less than annually, by the Information Security and Privacy Group (ISPG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the ISPG at mailto:ciso@cms.hhs.gov.