Centers for Medicare & Medicaid Services
Information Security and Privacy Group

Plan of Action and Milestones Process Guide

Final

Version 1.1

March 23, 2021

Record of Changes

The table below capture changes when updating the document. All columns are mandatory.

Version Number	Date	Chapter Section	Author/Owner Name	Description of Change
1.0	*10/20/2020*	*All*	*ISPG*	*Initial Version*
1.1	*03/23/2021*	*All*	*ISPG*	*Inclusive Language update*

Effective Date/Approval

This Procedure becomes effective on the date that CMS's Director, Division of Security and Privacy Policy and Governance (DSPPG) signs it and remains in effect until it is rescinded, modified or superseded.

Signature:	/S/	Date of Issuance	03/23/2021

Michael Pagels
Director, Division of Security and Privacy Policy and Governance (DSPPG) and Acting Senior Official for Privacy

Table of Contents

Tables

Figures

1. Introduction

The Centers for Medicare & Medicaid Services (CMS) has implemented an Information Security and Privacy Program to protect CMS information resources. One component of this program is the implementation of an effective Plan of Action and Milestones (POA&M) strategy. A POA&M is a corrective action plan for tracking and planning the resolution of information security and privacy weaknesses. It details the resources (e.g., personnel, technology, funding) required to accomplish the elements of the plan, milestones for correcting the weaknesses, and scheduled completion dates for the milestones as described in Office of Management and Budget (OMB) Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*.

The *Federal Information Security Modernization Act (FISMA) of 2014* [1]mandates that every federal agency and respective agency components develop and implement a POA&M process to document and remediate/mitigate program- and system-level information security weaknesses and to periodically report remediation progress to the OMB and to Congress. The Presidential Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure states that "Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies."[2] OMB has published various memoranda containing requirements to implement statutes and Executive Orders, and requires program officials to regularly update the agency Chief Information Officer (CIO) on the progress of POA&Ms so that the CIO can monitor remediation efforts and provide periodic updates to OMB. Thus, CMS must develop a POA&M for each system and each security/privacy program in accordance with the Department of Health and Human Services (HHS) *Information Systems Security and Privacy (IS2P) Policy* to track identified risks and weaknesses until remediated or mitigated.

This document supersedes the *Risk Management Handbook Volume III, Standard 6.2 Plan of Action and Milestones Process Guide*, dated November 5, 2015. It does not supersede any other applicable policy, standard, law, or higher level agency directive. All references noted are subject to periodic revision, update, and reissuance. The latest standard regarding POA&Ms from HHS is the HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting dated 06/03/2019, and updates HHS and CMS requirements for managing and reporting POA&Ms.

1.1 Purpose

The purpose of this document is to provide CMS with the guidelines for properly documenting and managing POA&Ms. This Plan of Action and Milestones Process Guide is designed to assist in effective management and mitigation of organizational risk. The purpose of this guide is to provide information security personnel and stakeholders with guidance to aid in understanding, developing, maintaining, and

[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 Executive Order (EO) highlights some Known vulnerabilities as using operating systems or hardware beyond the vendor's support lifecycle, failing to implement a vendor's security patch, and implement security-specific configuration guidance

reporting program, and system-level weaknesses and deficiencies to HHS. It also provides the necessary requirements and protection for all POA&M information that is properly managed and entered into the CMS FISMA Control Tracking System (CFACTS).

1.2 Background

The 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 and provides information for the E-Government Scorecard under the President's Management Agenda. 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 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. CMS accomplishes this task 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.

1.3 Scope

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

1.4 Applicability

This guide applies to all CMS FISMA information systems, 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, to include systems managed and/or operated by contractors and third-party service providers acting on behalf of CMS.

1.5 Definition

The POA&M is the corrective action plan (document or tool) for tracking and planning the resolution of the weaknesses. It details the resources (e.g., personnel, technology, funding) required to accomplish the elements of the plan, milestones for correcting the weaknesses, and scheduled completion dates for the milestones.

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

For the purpose of this document, the term "weakness" as defined in National Institute of Standards and Technology Special Publication 800-53, rev. 4, will be synonymous with the terms, finding, and vulnerability. These terms are defined below:

- **Finding –** Assessment and audit results produced by the application of an assessment and audit procedure to a security control, privacy control, or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition (Source: National Institute of Standards and Technology (NIST) SP 800-53A rev4). For this document, findings are referred to as weaknesses.
- **Vulnerability –** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (Source: NIST SP 800-53). For this document vulnerability and weakness are synonymous.
- **Weakness –** Refers to findings and vulnerabilities that require remediation. For this document, the terms weakness, deficiency, and vulnerability are similar; also weakness and finding are synonymous. For consistency, the term weakness is used throughout the document.

A POA&M is required for every system where an IT security or privacy weakness has been found. The findings may stem from internal or external audits, reviews, and Continuous Diagnostics 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 and tasks/steps, i.e., "milestones", 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 the risk to an acceptable level 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/approved and closed, the record must be retained for one year. Milestones should be S.M.A.R.T[4]:

- *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 in a CAP
- Assist agencies in reducing the risk of the identified weaknesses to an acceptable level, or closing their security and privacy performance gaps via mitigation or remediation
- 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 for supporting the federal cybersecurity and privacy programs

[4] See Appendix D for examples of inappropriate vs appropriate milestones

- Assist with Congressional oversight by providing pre-decisional budget information for supporting the federal cybersecurity and privacy programs

2. 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 ultimately with the CIO as the AO under FISMA. 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 U.S. federal 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].

3. POA&M Overview

The POA&M process is a methodical approach to overseeing the resolution of weaknesses and reducing or remediating 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 resources and financial costs for remediation, and provide a scheduled completion date. The plan is submitted to the Cyber Risk Advisor (CRA) for review. Once reviewed and approved, the Business Owner through the ISSO executes the plan and provides monthly updates into CFACTS to document the status of the mitigation efforts. The steps to the POA&M process[6] 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 Resource and Funding Availability
4. Assign a Scheduled Completion Date
5. Execute the Corrective Action Plan
6. Verify Weakness Completion
7. Accept the Risk When Applicable

[5] The CMS Policy for Information Security and Privacy Policy (IS2P2) (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.

[6] The CFACTS Manual is a useful guide for completing POA&Ms within the CFACTS tool. This can be found on the CFACTS Main page at https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx

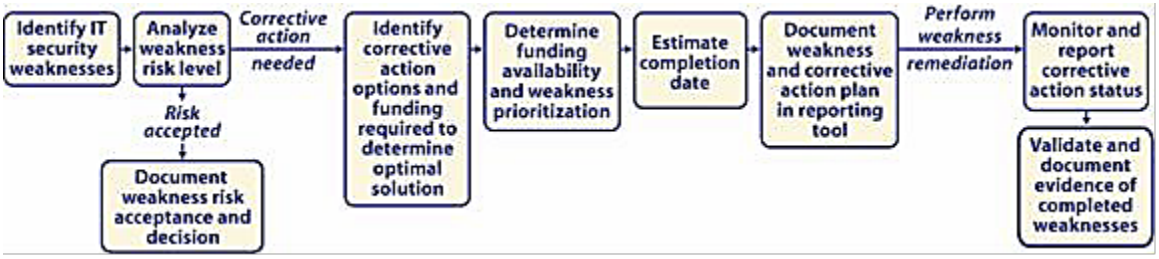

Figure 1. The Weakness Remediation Process

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 privacy of a system must be corrected and the required mitigation efforts are captured in the POA&M. A weakness arises from a specific 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 (vulnerability scans, penetration tests, etc.). 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 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 (SCA) or Adaptive Capability Testing (ACT)
- 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 Assessment and Audit Tracking (CAAT) template, and that the completed template is provided to ISPG for upload into the CMS POA&M CFACTS 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 SCA or ACT, 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 and reporting process. Typically, the assigned ISSO will have been delegated day to day responsibility for the assessment and creation of the CAAT template working with the independent third party assessor. 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.

As stated above, for the purpose of this document, findings and weaknesses are the same. Weaknesses may result from vulnerability scans, penetration tests, audits, security assessments, incident reports, etc. All weaknesses must be carefully evaluated to determine if they are truly a weakness. Upon positive identification, weaknesses shall be remediated or documented as POA&Ms[7]. Table 1 provides a list of the types of weaknesses.

Table 1. Weakness Types

WEAKNESS TYPE	DEFINITION	EXAMPLES
Program Weakness	A program weakness typically pertains to CMS enterprise-wide information security and privacy program. Program weaknesses are documented in a program-level POA&M and are addressed separately from individual system weaknesses. A program weakness can be tied to an enterprise-wide common control, e.g., NIST 800-53 Awareness and Training (AT)-1 control which requires an enterprise-level security awareness and training policy and procedures.	• Security policy is not updated with the latest NIST and OMB guidance. • Security awareness training has not been completed by all newly hired employees. • Security incidents are not appropriately documented and maintained in accordance with HHS policy.
System Weakness	A system weakness pertains to the management, operational, or technical controls of a specific system.	• Password length is not in compliance with HHS policy. • System changes are not appropriately approved prior to implementation. • System does not generate audit record. • System's sensitive data at rest is not encrypted.

[7] Any scan findings that are identified as false positive will be excluded from documenting a POA&M. False positive is defined as "An alert that incorrectly indicates that a vulnerability is present" (Source: NIST SP 800-115).

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).

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 2. 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 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.

Remember that risk can be evaluated either qualitatively or quantitatively and is typically expressed in its simplified form as:

***RISK* = THREAT x IMPACT x LIKELIHOOD**

The result of the analysis of the risk(s) from following the NIST SP 800-30 guide will recommend the overall risk level assigned to FISMA system of record.

3.1.5 Remediation/Mitigation Timelines

After positive identification of scan findings or approval of security assessment and/or audit report, all findings/weaknesses shall be documented in a POA&M, reported to HHS, and remediated/mitigated within the following remediation timelines.[8]

- Critical within **15 days;**
- High within **30 days;**
- Moderate within **90 days;** and
- **Low** within **365 days**.

Business Owners, ISSOs, and/or other POA&M stakeholders shall determine the scheduled completion date for each POA&M within the specified remediation timelines. These timelines are based on the Date Identified, not the date the POA&M is created. Stakeholders should complete and submit their CAAT templates in a timely manner to allow for the maximum time to complete the remediation/mitigation.

If it is determined that additional time is needed to remediate/mitigate a weakness, the justification with a modified estimated completion date shall be documented in the POA&M in the Changes to Milestones and Comment fields. If weaknesses are not remediated within the scheduled completion date, the status shall change to "Delayed".

Government audit: Findings/weaknesses identified during a government audit (i.e., Inspector General or GAO audit) shall be documented in the POA&M after the audit draft report is produced, regardless of CMS acceptance of the identified weakness(es). Disagreements on findings that cannot be resolved between CMS and the auditing office shall be elevated to the Department for resolution.

Systems shall review and update POA&Ms **at least monthly**. In addition, compensating controls shall be in place and documented until weaknesses are remediated or mitigated to an acceptable level of risk.

3.1.6 Evaluating Weaknesses

All weaknesses shall be examined to determine their root cause prior to documentation in the POA&M. Proper evaluation ensures the cause, not the symptom, is treated and prevents resources from being expended unnecessarily on addressing the same weakness.

[8] Remediation refers to complete fix of a weakness; mitigation refers to remediating the weakness to an acceptable level of risk, but not fully resolved. NIST SP 800-53 defines risk mitigation as "Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process."

3.1.7 Prioritizing Weaknesses

CMS shall take a risk management approach and ensure that weaknesses of critical and high impact level take precedence over lower security weaknesses. CMS shall prioritize weaknesses on an ongoing basis to ensure that high-priority weaknesses receive the funding and the resources necessary to remediate/mitigate the most significant risks, since funding and assignment of resources to remediate/mitigate weakness may change over time.[9]

Table 3 below describes some weakness prioritization factors. Systems may define additional or different prioritization factors for consideration to better accommodate their environment.

Table 3. Weakness Prioritization Factors

PRIORITIZATION FACTOR	DESCRIPTION
Risk Level/Severity	Not all weaknesses represent the same risk level of the FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, system impact rating of the system on which it resides and/or the severity of the weakness itself. Weaknesses on a High or Moderate system or weaknesses that contribute to a material weakness, significant deficiency or reportable condition will normally require more immediate resolution. This prioritization factor must consider the following elements: • Sensitivity and criticality of information on the system, such as personally identifiable information (PII). • The estimated likelihood of the weakness occurring and/or being exploited. • The cost of a potential occurrence or exploitation in terms of dollars, -person-hours, and/or reputation.
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 authorization boundary? Is it a potential program weakness? Is the weakness a systemic issue (across the enterprise) or is it an isolated event? Systemic issues represent much greater risk and may, therefore, be a higher priority.
Source	What is the source of the weakness? For example, if the weakness resulted from an audit and is considered a significant deficiency, then greater attention should be focused on this weakness.
Visibility	Has the weakness drawn a high level of visibility external to the system or program? 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. Such weaknesses take priority above higher

[9] It is important to note that weakness evaluation and prioritization is an ongoing process. When a new, critical weakness is discovered, resources may need to be shifted to mitigate or remediate it appropriately. Therefore, weaknesses that were once deemed a high-priority may not necessarily be considered as such as time progresses and risks/threats change.

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, monitored, and worked to closure or risk based acceptance.

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 tasks/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 and resource requirements to remediate the weakness. Appendix D of this document provides samples of compliant and non-compliant milestones for use in documenting the CAP.

3.3 Determine Funding Availability

The system BOs, ISSOs, and/or other stakeholders shall ensure adequate resources are allocated to mitigate/remediate weaknesses and determine the funding and/or full-time equivalent (FTE) resources required to remediate/mitigate each weakness on the POA&M.[10] The resources required for weakness remediation shall fall into one of the following three categories:

- Using current resources allocated for the security and/or management of a program or system to complete remediation activities
- Reallocating existing funds that are appropriated and available for the remediation, or redirecting existing personnel
- Requesting additional funding or personnel

Duplicate or similar weaknesses shall be documented in one POA&M, existing or new, to avoid inconsistencies. If a related POA&M already exists, the additional weakness shall be noted in the comment field.

3.4 Assign a Scheduled Completion Date

System BOs, ISSOs, and/or other stakeholders shall determine the scheduled completion date for each weakness based on timelines required to determine the resources needed to remediate the weakness and within the remediation time limits described in Section 3.1.5. The milestone(s) completion date shall not exceed the scheduled completion date assigned to the weakness. It is also a good practice to first determine

[10] Making funding decisions is often a collaborative exercise that involves multiple system personnel and stakeholders. Examples of questions to ask are: Is one enough or will the participation of a larger team be needed? Can the task be accomplished within a week or will it take several months? How serious is the weakness? Other factors to consider are Complexity of the Corrective Action Plan (updating policy, changing code, etc.), purchasing requirement, risk level/severity (if required to remediate/mitigate immediately), etc.

the milestones with completion dates, as this will help determine a more accurate overall scheduled completion date for the weakness. The scheduled completion date established at the creation of the weakness **shall not** be modified after the weakness is reported to the OMB. POA&Ms become reportable once the status changes from "Draft" to "Ongoing". If a weakness is not remediated within the scheduled completion date, a new **estimated completion date** shall be determined and documented in the Changes to Milestones and Comment fields in the POA&M.

NOTE: In instances when the scheduled completion date will exceed the required HHS Remediation/Mitigation Timeline schedules, we strongly recommend you consider utilizing the Risk-Based Decision (RBD) process.

3.5 Execute the Corrective Action Plan

A designated Point of Contact (POC), responsible for ensuring proper execution of the corrective action plan, shall be identified for each weakness and its milestones. Individual(s) responsible for the execution of the corrective action plan vary widely depending on the organization, system, milestones, and weakness. This POC resource will be key to identifying an "owner" of the milestone and ensuring the milestone is worked to the eventual remediation of the weakness or acceptable mitigation of the weakness. Once the planning of the necessary corrective action is complete and adequate resources have been made available, remediation/mitigation activities shall proceed in accordance with the plan.

The completion of milestones provides a mechanism to demonstrate remediation/mitigation progress and identify potential delays to the overall completion of the corrective actions. If the completion of a milestone surpasses its original estimated completion date, an update to the milestone and the actual completion date of the milestone shall be captured in the "Changes to Milestone" field of the weakness in the POA&M. If the scheduled completion date has passed before the weakness is remediated/mitigated, the weakness shall default to "Delayed" status and a justification with a new estimated completion date shall be documented in in the "Comment" field and/or "Changes to Milestone" field of the relevant weakness.

3.5.1 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 at a minimum 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

3.5.2 Weakness Status

A weakness status must be assigned to each corrective action to denote progress toward remediation/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. POA&M 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. Any removal of a POA&M must happen during this timeframe. After 30 calendar days, the POA&M status will be automatically changed to Ongoing/Open; a scheduled completion date commensurate with the weakness risk level will be automatically assigned to it and will be reported to HHS.
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 remediated/mitigated. Documentation is required to demonstrate the weakness has been adequately resolved, including the date of completion.
Pending Verification	Indicates that all milestones/corrective actions have been completed but require review and sign-off to ensure an 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. An acceptance of the risk must be certified by the AO and documented accordingly via the RBD process. The weakness and corresponding risk must be monitored periodically, but no less than annually, to ensure the associated risk remains at an acceptable level. This status will be assigned automatically once the RBD has been signed by the AO.
Audit Approved	Indicates that a Completed POA&M has been audited by a member of the CISO's office or an independent third party and has been verified to be remediated/mitigated.
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 auditor has determined that the weakness has NOT been verified as remediated/mitigated and still remains "other than satisfied" as a weakness. The individual responsible for the POA&M will be required to reconcile any noted discrepancy identified by auditor.

3.6 Verify Weakness Completion

OMB's FISMA reporting guidance recommends that weaknesses should be considered "Completed" only when fully resolved. The ISSO will provide evidence and proof 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. Completed POA&Ms shall remain on the POA&M report for **one year from completion date**. The artifacts are stored in CFACTS and retained for at least one year with the completed POA&M.

NOTE: For systems that have been decommissioned, the status of associated weaknesses in the POA&M document shall be changed to "Completed" or transfer all POA&Ms that are applicable to other systems with an annotation that the system has been decommissioned. The POA&M no longer has to be tracked.

3.7 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 AO or CIO, who may make the decision to accept the risk at their discretion. After approval, RBDs shall be reviewed **at least annually** to ensure the risk remains acceptable and updated as events occur and information changes.

4. 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. CMS shall submit POA&M updates at least **once a month** (**by the 3rd business day of each month**) to HHS to demonstrate the status of POA&M mitigation/remediation activities.

CMS shall submit the following information in accordance with the Department POA&M reporting requirements:

- All POA&Ms associated with a program, system and/or component that are within an authorization boundary. POA&Ms shall be tied to the individual system and/or component and not the authorization boundary.
- An explanation associated with each delayed POA&M and a revised estimated completion date.
- Completed POA&Ms for up to one year from the date of completion.

5. CFACTS

Stakeholders must use CFACTS to identify, track, and manage all IT system weaknesses and associated POA&Ms to closure for CMS information systems. 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, HHS, and CMS requirements. Support for CFACTS and offline copies of the User Manual are available by emailing the CISO mailbox.

Appendix A. Acronyms

Acronym	Meaning
AO	Authorizing Official
BO	Business Owner
CAAT	CMS Assessment and Audit Tracking
CAP	Corrective Action Plan
CFACTS	CMS Federal Information Security Modernization Act Control Tracking System
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
CRA	Cyber Risk Advisor
HHS	Department of Health and Human Services
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
ISPG	Information Security and Privacy Group
ISSO	Information Systems Security Officer
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact

Acronym	Meaning
RBD	Risk-Based Decision
RCA	Root Cause Analysis
RMF	Risk Management Framework
RMH	Risk Management Handbook
RVA	Risk and 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 B. Glossary

Term	Definition
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.
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 includes 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 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.

Term	Definition
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.
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 C. References

Federal Laws

Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

DHS

DHS Binding Operational Directive (BOD) 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, April 29, 2019, https://cyber.dhs.gov/assets/report/bod-19-02.pdf

NIST Standards and Special Publications

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*, March 2006, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

NIST Interagency or Internal Report (NISTIR) 7298, *Glossary of Key Information Security Terms*, Revision 2, May 2013, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, Revision 1, February 2006, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

NIST SP 800-30, *Guide for Conducting Risk Assessments*, Revision 1, September 2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Revision 1, June 5, 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*, March 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*, Revision 3, July 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Revision 4, December 2014, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

NIST SP 800-60 Volume 2, *Guide for Mapping Types of Information and Information Systems to Security Categories, Appendices*, Revision 1, August 2008, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-65.pdf

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, May 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

NISTIR 7298, *Glossary of Key Information Security Terms*, rev.2, June 2013, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

OMB Circulars/Memoranda and EOs

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*,

July 15, 2016, https://www.whitehouse.gov/omb/information-for-agencies/circulars/

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, https://www.whitehouse.gov/omb/information-for-agencies/circulars/

OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001, https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2002

OMB Memorandum 14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013, https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2014

OMB Memorandum 16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016, https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2016

OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017, https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2017

OMB Memorandum 19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and PrivacyManagement Requirements*, October 25, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/10/M-19-02.pdf

Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

HHS Policies Standards and Guides

Departmental Security Policy and Standard Waiver/Risk Acceptance Form, June 21, 2016 https://community.max.gov/download/attachments/1205537135/HHSWaiver-RiskAcceptanceForm21June2016.pdf?version=1&modificationDate=1517348480390&api=v2

HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance, July 15, 2016, https://intranet.hhs.gov/it/strategy-policy-governance/policies-standards-guides/memoranda/index.html

HHS Information Systems Security and Privacy Policy (IS2P), July 30, 2014, https://intranet.hhs.gov/it/strategy-policy-governance/policies-standards-guides/policies/index.html

Resolving Security Audit Finding Disputes, May 13, 2010, http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/SAFD/hhs_ocio_memo_resolving_security_audit_finding_disputes_05132010.pdf

Other

FedRAMP Plan of Action and Milestones (POA&M) Template Completion Guide, February 21, 2018, https://www.fedramp.gov/assets/resources/documents/CSP_POAM_Template_Completion_Guide.pdf

Business Requirement Document: Archer HHS Assessment and Authorization, https://community.max.gov/display/HHS/First+Iteration+Notional+Deployment+Materials

HHS SGRC Lexicon, June 22, 2018, https://community.max.gov/display/HHS/Lexicon

U.S. Government Accountability Office (GAO) *Green Book*, September 20, 2014, https://www.gao.gov/greenbook/overview

Appendix D. Sample Milestone Descriptions

A milestone is a specific, action-oriented step necessary to aid in the mitigation/remediation of a weakness. Each POA&M shall have at least one milestone associated with its mitigation/remediation, along with a completion date. Moreover, milestones shall be clear and effectively describe the major steps required to remediate the weakness. Table 5 below provides a few examples of appropriate and inappropriate milestones.

Table 5. Examples of Inappropriate vs. Appropriate Milestones

POA&M DESCRIPTION	EXAMPLE	MILESTONES WITH COMPLETION DATES
Vulnerability scanning does not incorporate the entire environment as documented in the System Security Plan.	Inappropriate	1. Ensure vulnerability scanning covers the entire environment; (11/15/2018)
Vulnerability scanning does not incorporate the entire environment as documented in the System Security Plan.	Appropriate	1. Schedule a review of the environment inventory; (11/15/2018) 2. Update the System Security Plan and the vulnerability scanner to reflect the updated inventory; (1/31/2019) 3. Conduct a vulnerability scan to check that the entire inventory is included; (2/15/2019) 4. Implement an ongoing process to evaluate and update the inventory, the System Security Plan, and the vulnerability scans on a regular basis; (3/15/2019) 5. Perform a vulnerability scan and cross check the output with the updated inventory list to verify that the entire environment is included; (4/15/2019)
Audit logs are not periodically reviewed.	Inappropriate	1. Ensure that audit logs are periodically reviewed; (12/15/2018)
Audit logs are not periodically reviewed.	Appropriate	1. Review policy to ensure that audit log review is required; (12/15/2018) 2. Identify the SO; (12/16/2018) 3. Establish communication and training to convey the requirement of audit log review; (2/28/2019) 4. Schedule a follow-up review with the SO to ensure that audit log review is taking place. (3/31/2019)