Homeland
Security

U.S. Department of Homeland Security

DHS 4300A,

"Information Technology System Security Program,

Sensitive Systems"

Attachment H

Plan of Action and Milestone (POA&M) Guide

Version 3.0
July 28, 2022

Protecting the Information that Secures the Homeland.

Document Change History

Version	Date	Description
2.0	May 13, 2022	Form redesigned. Instructions updated to align with 4300A Policy updates and current processes. Prepared document for review by the SMEs.
3.0	July 28, 2022	Comments Adjudicated by CISOD Compliance Division.

Table of Contents

Note: *When in hard copy, this document is not a controlled copy and does not necessarily reflect the latest version. This is a living document and will be subject to change due to revisions in plans, funding availability, or other factors.*

1.0 INTRODUCTION

The Department of Homeland Security (DHS) Chief Information Security Officer Directorate (CISOD) is responsible for initiating and administering an information security program to protect its information resources in compliance with applicable laws, regulations, and Executive Orders.

The Federal Information Security Modernization Act of 2014 (FISMA)[1], mandates that all Federal departments and agencies develop and implement a corrective action plan, known as a Plan of Action and Milestones (POA&M) and periodically report progress of these remediation efforts to the Office of Management and Budget (OMB).

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*.

Effective POA&M management increases the awareness of the government's security posture, contributes to development of risk–based decisions, and assists organization leadership to prioritize resource allocation. All identified security and privacy weaknesses shall be recorded and managed via POA&Ms.

1.1 Authority

The Chief Information Security Officer Directorate (CISOD) is responsible for overseeing the cybersecurity and risk management of DHS's and Components Information Systems. The DHS CISO shall ensure that Information Technology (IT) security policies and requirements are consistent with applicable statutory authority, FISMA, Federal policies, Office of Management and Budget (OMB) mandates[2], and DHS policies and Instructions in balance with Component mission needs. This responsibility includes the delegated authority to develop, implement, and manage a DHS-wide POA&M process.

DHS and Components shall document, maintain, and report POA&Ms using the designated agency system of record, DHS' Information Assurance Compliance System (IACS), Cyber Security Assessment and Management (CSAM) tool. Components are required to manage POA&Ms and supporting artifacts to reflect their remediation efforts in CSAM. DHS reviews and analyzes the information in CSAM for reporting and decision-making purposes. POA&M information that is needed for audit responses will be pulled from CSAM as the system of record.

[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] M-02-01, Memorandum for the Heads of Executive Departments and Agencies "Guidance for Preparing and Submitting Security Plans of Action and Milestones," https://obamawhitehouse.archives.gov/omb/memoranda_m02-01/

FISMA requires that each POA&M be tied to the planning Agency's budget submission. Reporting on IT investment is required by OMB to identify the costs of providing IT security as part of the investment life cycle, and to identify IT security costs for supporting infrastructure-related investments under FISMA.

Capital Planning and Investment Control (CPIC) process is required by legislative authorities and requirements from the Clinger-Cohen Act to comply with the budget preparation guidance provided by OMB Circular A-11 and A -130. Policy direction and process for DHS is provided by Management Directive 102 – Acquisition Management and Management Directive 1330 on Planning, Programming, Budgeting and Execution (PPBE). More information can be found on the Enterprise Business Management Office (EBMO) site through DHS Connect.

1.2 Purpose

The purpose of this POA&M Guide is to outline the requirements for developing, maintaining, closing, and reporting program and system-level weaknesses and deficiencies to DHS for all information systems and programs supporting DHS. The information provided in this Guide is applicable to all DHS information systems including contractor-operated DHS information systems (i.e., systems that are DHS-owned but operated by contractors) and externally operated or hosted information systems (i.e., systems managed or hosted outside of DHS environments, including cloud systems), that collect, store, process, or transmit DHS information. In this guide, *system* refers to any systems listed in the DHS FISMA system inventory to include systems managed and /or operated by contractors as well as third-party service providers such as Cloud Service Providers (CSPs) acting on behalf of DHS. It also provides the necessary requirements and protection for all POA&M information that is properly managed and entered into CSAM.

In accordance with all agency requirements, POA&Ms must be developed to track identified risks and weaknesses until mitigated or remediated. At a minimum, System Owners or a designee(s) must review POA&Ms on a monthly basis. The DHS Information Security Performance Plan (ISPP) provides the criteria for specific metrics for Weakness Remediation on the FISMA Scorecard.

This POA&M Guide is not intended to be a CSAM user manual.

All references noted throughout this document are subject to periodic revision, update, and reissuance.

1.3 Roles and Responsibilities

The overall responsibility for POA&Ms rests ultimately with the DHS CIO as the AO under FISMA. By authority of the DHS CIO, the DHS Chief Information Security Officer Directorate (CISOD) is assigned responsibility for implementing and managing the Department's Information Security Program and for ensuring compliance with FISMA, OMB, and other Federal requirements relevant to information security. The CISOD 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 Owners, and the Information System Security Managers and 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 DHS may assist in the performance of security and privacy functions.

The DHS Cybersecurity Risk Management and Compliance (CRMC) Division will conduct periodic reviews and quality checks of Components POA&Ms to ensure that requirements are being met. It is up to CRMCs discretion to request a Component to amend, open or cancel a POA&M if it is found to be invalid, incorrect, or insufficient.

For further information on Roles and Responsibilities, *see Attachment W, Roles and Responsibilities.*

1.4 System of Record

CISOD understands that some Components may employ ancillary solutions to track weakness remediation efforts associated with POA&Ms. To ensure FISMA reporting compliance, DHS and Components shall identify, track, and manage all IT program and system weaknesses POA&Ms using the designated agency system of record, CSAM.

While CSAM provides multiple options for many of the field types described in this document, only those which are explicitly described will be accepted within CSAM.

2.0 TYPES OF POA&Ms

All DHS FISMA systems are required to develop, manage, and maintain a corresponding POA&M for identified vulnerabilities. Findings requiring POA&Ms on Subsystems and Minor Applications are required to be tracked and remediated through the parent information system’s POA&Ms.

- **Program Level POA&Ms** – A Program Level POA&M is created to assist in documenting findings and vulnerabilities at the program or DHS organization level which affect the programs or organization’s IT security efforts.

- **System Level POA&Ms** – A System Level POA&M assists in documenting planned remedial actions to correct findings and vulnerabilities identified in relation to the technical, management, or operational aspects of a DHS information system, IT resource, or controls in NIST SP 800-53, Revision 5.

3.0 POA&M CONTENT AND PROCESS

The POA&M process consists of the following activities:

- Identify and document weaknesses
- Determine the severity level of the weakness in order to prioritize POA&M efforts according to risk factors
- Determine responsibility
- Estimate cost as a line item in the POA&M ONLY if a purchase of equipment, software licenses, or training, etc., is required for POA&M remediation. The man hours of existing personnel who remediate patches or configuration issues need not be “costed” as they are already budgeted for this work. If “other” costs are required, include a description for costing in the line items (milestones) of the POA&M for this purpose.

Due to the length of time purchasing requires, it may become necessary to risk adjust through the implementation of countermeasures and a "waiver" may need to be submitted for a delayed remediation.

- Develop a Remediation Plan by:
  - Identifying the root cause of the weakness or vulnerability
  - Identifying compensating controls that should be implemented to reduce risks until the control can be fully remediated
  - Identifying resources needed to resolve the weakness
  - Developing steps/milestones needed to resolve the weakness (at least 2 milestones are required for all POA&Ms) that should be clearly identifiable, easily measurable, and have achievable completion dates
  - Take the corrective actions needed to resolve the weakness and implement the plan
  - Monitor and update the POA&M as needed
  - Report status of weaknesses to DHS and government-wide authorities at specified intervals

3.1 Weakness Identification

A weakness is any information security vulnerability or finding that could compromise the confidentiality, integrity, or availability of an information system. The identification of a weakness results from security assessments, vulnerability and penetration tests, security audits such as the FISMA audit, Office of the Inspector General (OIG) audits, Financial Statement audits, Government Accountability Office (GAO) audits, or any other internal or external assessment or vulnerability scans.

3.1.1 Security Assessments

Weaknesses identified and documented in the approved signed Security Assessment Report (SAR) must have corresponding POA&Ms in CSAM if the finding is not remediated within 30 calendar days. Any controls receiving a result of Not Tested or Not Satisfied will be recognized as a risk to the system and a POA&M generated if not remediated within 30 days. A new POA&M should only be created for new findings. Repeat Findings must be tracked as part of the existing original open POA&Ms. The existing open (original) POA&M may not be closed or cancelled unless evidence of closure can be validated by the designated ISSM accordingly.

3.1.2 Vulnerability and Penetration Tests

In addition to the aforementioned stipulations for creating a POA&M (in section 3.1.1 Security Assessments), Components that undergo a vulnerability and penetration test engagement, have a Vulnerability Disclosure Program (VDP) finding, or a finding during a Hack DHS Bug Bounty event with the Department of Homeland Security (DHS) Vulnerability Assessment Branch (VMB) Penetration Testing Team (PTT) or Vulnerability Assessment Team (VAT) must associate and document any identified vulnerabilities with a POA&M in the DHS Cybersecurity Assessment and Management (CSAM) application. This policy also applies to findings resulting from Components hosting their own Bug Bounty, who procure penetration testing services through other government vulnerability discovery and penetration testing teams, or who procure third-party vulnerability discovery and penetration testing services.

In the case of assessments in which a technical report is a final deliverable, a POA&M is not required if remediation can be completed before the final report is completed and recorded in said technical report. In the case of Bug Bounty events, if POA&M requirements and process are defined in the Rules of Engagement they will supersede the above paragraph, but any findings not remediated findings at the end of the engagement must have a POA&M created in CSAM.

3.1.3 Risk and Vulnerability Assessments and Security Architecture Reviews for High Value Assets

In May 2018, DHS released Binding Operational Directive BOD 18-02, "Securing High Value Assets." This BOD includes Risk and Vulnerability Assessments (RVAs) and Security Architecture Reviews on HVA systems for all High Value Assets in the Federal Government enterprise. Within 30 days of receipt of an RVA or Security Architecture Review report identifying a major or critical weakness in an assessed HVA, a corresponding POA&M must be created in CSAM. If it is determined by the designated Senior Accountable Official for Risk Management (SAORM) that full remediation cannot be completed within the initial 30-day timeframe, or timeframe prescribed by the criticality of the weakness, whichever is sooner, the remediation plan must be developed and submitted to the DHS HVA POC for each HVA with remaining major or critical weaknesses within 30 days of receipt of the RVA or Security Architecture Review. The POA&M remediation plan must be updated in CSAM every 30 days until full remediation is achieved for all assessed HVA.

BOD 18-02 requires RVA and Security Architecture Review remediation plans to be reviewed and approved by the agency designated SAORM prior to submission to DHS HVA POC. The notifications for modifications and POA&M full remediation must be certified and signed by the designated SAORM.

The DHS HVA POC will centrally manage POA&M progress and report submissions and will engage each Component in all cases where the Agency has not met POA&M remediation Schedule Completion Dates (SCD).

3.2 POA&M Development

If remediation of a weakness cannot be resolved within thirty (30) days of discovery, or within the timeframe prescribed by the criticality of the weakness, whichever is sooner, Components must create a POA&M in CSAM to track the open finding or vulnerability. **Refer to section 3.1.1-3.1.3 for additional guidance on weaknesses identified through assessments and testing.**

Key stakeholders must determine resources required including costs, milestones, prioritization, and any other pertinent items that will affect remediation and/or mitigation activities. Once all required fields in CSAM are complete for each POA&M, the ISSM shall approve the draft POA&M. *Note:* CSAM will automatically approve a POA&M that remains in "draft" status for a period of thirty (30) days and will be accounted for in the Systems Weakness Remediation Score. During the first 30 days in draft this POA&M will not be accounted for in the systems Weakness Remediation score.

3.3 POA&M Title

Each POA&M should have a unique, clear, and concise title. A POA&M title should be indicative of the weakness. For all POA&Ms associated with OIG audits or GAO engagements, the POA&M title must contain the Notice of Findings and Recommendations (NFR) number, Title/Report number, and Title. If the weakness exists for a subsystem or minor application, ensure the subsystem/minor application is listed in the title.

3.4 Weakness Description

POA&M descriptions must provide a complete and accurate description of the identified weakness and provide sufficient information to facilitate oversight and progress tracking. DHS CISOD expects Components to document this field with detail sufficient for an individual who is not familiar with the weakness to understand it. The description succinctly states why the identified weakness does not meet the control-requirement. Avoid repeating a generic control statement, as this does not accurately describe an observed weakness.

Any POAM resulting from an audit finding shall include the exact language from the formal recommendation along with the report and recommendation number (FISCAM, FISMA, or GAO engagement, etc.).

3.5 Criticality

The NIST Special Publication (SP) 800-30 Revision 1, "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.

CSAM automates the weakness criticality assignment based on the assessment and risks associated with all controls referenced within the POA&M in question.

In the case that CSAM does not provide a CSAM derived criticality, the criticality identified in the POA&M should be reflective of what is listed in the authoritative source that identified the risk. Examples of authoritative sources are Security Assessment Reports, Common Vulnerabilities and Exposures (CVEs), Information Security Vulnerability Management (ISVMs).

CSAM allows the System Owner and/or ISSO to define criticality in POA&Ms as: (1) Low; (2) Medium; (3) High. The User Identified Criticality assists Components with identifying remediation priority and resource allocation.

Criticality	Definition
Low	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Medium	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
High	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.

3.6 Determine the Root Cause

Root cause analysis is a structured systems analysis methodology that identifies the underlying causes of problems, issues, and or events. The goal of root cause analysis is to identify the underlying problem(s) and their solution(s) by attempting to set bounds for, correct, or eliminate underlying causes, as opposed to addressing the immediately obvious symptoms. In performing a root cause analysis, the policy, procedures, people, technology, and resources relevant to the identified security weakness are reviewed because inadequacies in one or more of those areas are generally the root cause(s) of the weakness. ***The root cause for each POA&M must be documented in the comments section of the POA&M in CSAM.***

Reasons for conducting root cause analysis include:

- It helps System Owners and stakeholders understand information security impact to mission and operations.
- It helps System Owners, responsible system admins, and Information System Security Officers (ISSO) with assignment of risk and subsequent prioritization for remediation.
- It helps identify underlying causes of control weaknesses that are exacerbating issues that are preventing a control from working as designed and implemented. The root cause also assists with the broader need of creating the steps in the remediation plan for the underlying finding or vulnerability.
- Documenting root causes provides a broader understanding of control gaps.
- It can reduce the likelihood of control recurrence by focusing corrective actions on the cause (finding, vulnerability, gap, etc) rather than the systematic symptoms. which are more frequently reported.

The following steps are recommended when conducting a root cause analysis:

- **Understand the impact of the identified problem** (e.g., a security control weakness) on business or mission needs. Do not focus on the symptoms or technology issues; first try to understand the problem in its entirety. Do not start investigating possible solutions until the problem is bound and defined from the expert, process, and technology perspectives. Otherwise, the solution may bias the root cause analysis.

- **Consider the known threats and vulnerabilities** associated with the security control weakness, and understand the risk to, and impact on, the organization, location, program or project, system, and data and information.
- **Review the latest applicable control procedures** given in the current revision of NIST SP 800-53 to determine if the procedures are understood and the expected control design and implementation is documented in the System Security Plan (SSP). Determine whether the control is considered a critical "key control." Review the underlying security requirement independent of the solution — and evaluate functional control requirements for quantity, quality, coverage, timelines, and availability.
- **Review existing business processes or standard operating procedures (SOP)**. Consider business-process descriptions and compensating controls. Are they part of the documented security control design and implementation requirements?
- **Review the Systems Technology**, including security architecture and security services being used to implement and support the control. Determine whether the hardware platform, operating system (OS) and application software are adequate to meet the internal control design and implementation requirements.
- **Identify the People** who are responsible for developing, implementing, documenting, testing and continuously monitoring the security control (e.g., system owners, responsible system engineers, ISSOs, supervisors, etc.). Determine if they are aware of and understand the procedures, they are responsible for executing. Has the staff been sufficiently trained, and do they follow the procedures?
- **Identify the Resources** needed to properly implement and monitor the internal control (including people, hardware, software licenses, software development time, implementation, test, documentation, training, and continual monitoring of effectiveness). Is the solution achievable with current resources (staff, funding, and systems) during the next six to 12 months, or does the system owner or other principal stakeholder (e.g., Component CIO, CFO) want to consider a waiver request? Is the remediation or mitigation activity (the solution) cost justifiable? Root cause analysis should determine if current resources can address the control weakness or if additional longer-range funding for resources should be requested (e.g., OMB Exhibit 300 funding requests, etc.).

Common root causes include the following:

- Written policy and/or procedures are lacking.
- Component policies are inaccurate, or otherwise inadequate.
- SOPs are not being followed; instead, emergency fixes are being applied with no record of change management approval.
- Notification of critical security patches is not being received by the Operations Staff, or implementation is not ensured by tracking.
- There is poor or inconsistent communication between the System Owner, ISSO and system engineers and the system operator.
- The hardware platform has reached end-of-life and is no longer being upgraded; only basic hardware maintenance activities are supported.
- The operating system does not include configuration management for hardening.
- Insecure services or default accounts need to be removed.

- Security log files not turned on or being overwritten.

3.7 Cost

Only when a POA&M requires a purchase to complete the remediation of a finding or vulnerability should line items be added to the POA&M instructing the System owner, responsible system admin, or other designated personnel to determine the cost in order to purchase the required materials for the remediation of the weakness. DHS CISOD expects components to work with personnel familiar with the program/system (system owner, responsible system admin, etc) and the weakness in estimating funding sources and costs. Costs can include hardware, software, licenses, training, travel and support and maintenance fees, as applicable. “Funding Resources” must be entered as a dollar amount. After implementing an appropriate counter measure for a finding or vulnerability, the system owner, responsible system admin, and other designated personnel must submit a “waiver” for the POA&M, for up to 12 months, to complete the remediation due to the purchasing requirements.

If the cost to remediate is not feasible or a technical remedy is not immediately possible, System Owners shall submit a waiver request for the remediation to be completed within 12 months. Otherwise a risk acceptance memo will need to be submitted for approval by the DHS CISO and AO.

3.8 Point of Contact

Planning to resolve a finding or vulnerability is dependent on the complexity of the security gap or weakness; as well as the criticality of the impact to the mission and system. To begin the process, a Point of Contact (POC) must be identified and entered in the ‘Assigned” field. The POC is usually the system engineer for the system affected but could also be anyone who has in depth knowledge of the system and has the capability to perform the tasks that need to be accomplished for weakness remediation. Search for the CSAM POC in the “Assigned” box and ensure the name, telephone number, and email address of the individual are included.

System Owners, or their designees, are responsible for updating POA&M POC information in CSAM as necessary It is imperative that the System Owner, responsible system admin, and/or their designee (ISSO/ISSM), verify on a regular basis that the POA&M POC is accurate and serves in such a capacity that will allow the System Admin responsible for the normal maintenance on the affected system, to plan remediation steps and milestones, and remediate the POA&M.

3.9 Scheduled Completion Date

All POA&Ms must include a Scheduled Completion Date. In accordance with OMB requirements, once a user assigns a Scheduled Completion Date for a POA&M, it cannot change. Upon POA&M approval by the ISSM, CSAM will lock the field. Providing an accurate estimate of completion is a critical task and requires consultation with the System Owner, Responsible System engineer (System Admin), Authorizing Official (AO), or other stakeholders as necessary. The completion date for resolving the weakness should be reasonable and should take into consideration the time necessary to perform a root cause analysis, to plan corrective action, to allocate the needed personnel resources and to complete the corrective action. Any additional needed costs should be included as a line item in the POAM for costing to affect the purchase of any needed items for remediation to take place. If any delays arise in completing the POA&M, users shall select a “Delay Reason” in CSAM via the drop-down menu and apply for a waiver to schedule the delayed remediation of the POA&M.

System Owners, Responsible System Admins, and/or other POA&M stakeholders shall determine the Scheduled Completion Date for each POA&M within the specified policy remediation timelines. ISSO's shall track the progress on the completion of POA&Ms and ISSMs shall perform POA&M closure only when there is evidence provided that the remediation is complete. Additionally, DHS shall take a risk management approach and ensure that weaknesses of critical and high impact level take precedence over lower security weaknesses, thus, remediated in a timely manner.

All open POA&Ms shall be tracked on the Weakness Remediation Scorecard, including ISVMs, and the required timeline for remediating vulnerabilities outlined, unless otherwise noted in FISMA 2014, are as follows:

- Critical vulnerabilities associated with Internet-facing systems must be remediated within 15 days of initial detection. [e.g. Binding Operational Directive (BOD) 19-02 (April 29, 2019)]
- High vulnerabilities associated with DHS internal systems must be remediated within 30 calendar days of detection.
- Moderate vulnerabilities associated with DHS internal systems must be remediated within 90 calendar days of detection.
- Low vulnerabilities associated with DHS internal systems must be remediated within 180 calendar days of detection.

POA&Ms with an overdue Scheduled Completion Date will fail the *Quality Check* on the Weakness Remediation Metric on the FISMA Scorecard.

3.10 Planned Start and Finish Dates

System Owners, or their designees, must provide a "Planned start and Finish Date" for each POA&M in CSAM. This differs from the POA&M completion date, and CSAM allows updates to these fields.

- **Planned Start Date** This is the day that the first milestone is intended to begin.
- **Planned Finish Date** This is the day that the last milestone is expected to be completed

3.11 Actual Start Dates

System Owners, responsible system admins, and their designees, must also provide the actual start date of initiated remediation activities for resolving the weakness. This field helps track and validate planning assumptions and will help improve future remediation forecasting.

3.12 Associations

System Owners, ISSOs or their designees are responsible for associating all POA&Ms with a security boundary, security unique finding/control or program. A single POA&M can associate or link to multiple security and privacy controls (multiple CVEs covering a unique finding or vulnerability) and does not require multiple POA&Ms in CSAM. However, the weaknesses should relate to each other and remediation activities can resolve multiple weaknesses.

Multiple findings should be consolidated into a singular POA&M if the findings will be remediated through the same series of remediation actions. If it is found that POA&Ms have been consolidated that should not be, a request to open additional POA&Ms will be made.

3.13 Milestones and Milestone Completion Dates

All POA&Ms must include milestones that outline the specific steps necessary to correct the identified weaknesses. All POA&Ms must have at least two milestones. All milestones must include a scheduled completion date, point of contact, milestone description, planned start and finish date, and an actual start date. System Owners, responsible System Admins, and their designees, shall provide discrete milestones that outline the specific remediation steps or objectives to address the weakness. Milestone dates should not all be the same because all activities would not begin and end at the same time.

It is essential that the milestone descriptions are consistent with the actions required to remediate the weakness. Milestones are the steps required in the remediation process, whether these are software updates or configuration changes, the steps for completing the remediation must be outlined with the Milestones (step dates). Milestone descriptions should not simply repeat a description of the weakness. Milestones should be:

- *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.

DHS CISOD requires Components to upload artifacts to each POA&M in CSAM as evidence of the completion/remediation of the weaknesses and corresponding milestones.

Below are examples of sufficient 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; (11/15/2021)
Vulnerability scanning does not incorporate the entire environment as documented in the System Security Plan.	Appropriate	1. Schedule a review of the environment inventory; (11/15/2021) 2. Update the System Security Plan and the vulnerability scanner to reflect the updated inventory; (1/31/2022)

		3. Conduct a vulnerability scan to check that the entire inventory is included; (2/15/2022) 4. Implement an ongoing process to evaluate and update the inventory, the System Security Plan, and the vulnerability scans on a regular basis; (3/15/2022) 5. Perform a vulnerability scan and cross check the output with the updated inventory list to verify that the entire environment is included; (4/15/2022)

3.14 Remediation/Mitigation Timeliness

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 DHS, and remediated/mitigated within the following remediation timelines.

- Per Binding Operational Directive (BOD) 19-02, "Vulnerability Remediation Requirements for Internet-Accessible Systems."
  - Critical findings or vulnerabilities must be remediated within 30 days or a POA&M must be created.
    - If a patch for a critical finding does not exist, it is advised that the responsible system admin create a countermeasure and POA&M the finding as a vendor dependency, risk adjusting the POA&M as a Deviation request based on the vulnerability and countermeasure implemented. ISSOs are responsible for following up with the vendors on a monthly basis following the approval of the Vendor Dependency POA&M in order to ensure the patch is applied as soon as it is available.
- Systems that are **internal facing:**
  - Critical and High findings or vulnerabilities must be remediated, or a POA&M must be created within 15 and 30 days if deviation for POA&M risk adjustment is approved or the remediation requires a purchase for the remediation, or other applicable issue, and a waiver has been approved for the delayed remediation, with appropriate counter measure implemented as a part of the POA&M for the risk adjusted remediation timeline.

3.15 POA&M Review and Tracking

The monitoring of POA&Ms is critical to maintaining a transparent view of security control status and posture across the enterprise. It is imperative that Components ensure a POA&M has quality and accurate content, schedule dates are attainable, resources are sufficient, and remediation actions are executable to address the weakness.

System Owners and ISSOs should review POA&Ms on a monthly basis and enter ‘notes’ in the POA&M milestones as updates become available in order to track remediation progress and as part of continuous monitoring.

The Weakness Remediation metric on the DHS FISMA Scorecard measures the key aspects of POA&M compliance, quality, and effectiveness. Details on how the Weakness Remediation metric is scored can be found in the ISPP.

DHS CISOD will monitor the creation and management of POA&Ms for compliance with this guidance. DHS CISOD will contact Component Compliance Designees and POA&M Managers with any questions and for status updates.

3.16 POA&M Workflow 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. Findings and vulnerabilities have 30 days to be remediated BEFORE a POA&M must be submitted for remediation. Detailed descriptions of various statuses are summarized in the following table:

Draft	Indicates that a weakness requires review and approval prior to “official” entry in the POA&M. If, after 30 days, a finding or vulnerability (Low, Mod, High) is NOT remediated the POA&M must be created and once submitted, will show a status of Ongoing or Open; a scheduled completion date commensurate with the weakness risk level will be automatically assigned to it, unless a Deviation Request (DR) is approved for Risk Adjustment (RA). A DR RA must be justified with the implementation of a countermeasure to be approved.
Completed	Assigned when all corrective actions have been completed or closed for a weakness and the weakness has been verified as successfully remediated/mitigated. Evidence documentation is required to demonstrate the weakness has been adequately resolved, including the date of completion. Evidence demonstrating the weakness has been resolved, see NIST SP 800-53A for acceptable evidence, is required to be uploaded in CSAM as an artifact to the POAM.
POA&M Close Requested	Indicates that all milestones/corrective actions have been completed but require evidence review and sign-off by the ISSM to ensure an effective resolution.
Late POA&M	Assigned when a weakness continues to be mitigated after the original scheduled completion date has passed. When the status changes to “late”, these will need to be reported to the FISMA Scorecard team and

	an explanation for why the POA&M has not been remediated provided to the FISMA team.
Waiver	If a POA&M requires a purchase, or other issue such a required purchase to remediate, the System Owner and Component CISO may waiver the finding or vulnerability in order to create a longer-term plan, of up to 12 months, for the remediation of the POA&M.
Risk Accepted	Indicates that the weakness risk has been accepted. An acceptance of the risk must be certified by the DHS CISO and Component AO and documented accordingly via the Risk Acceptance memo approval process. The weakness and corresponding risk must be monitored at least annually, or at the annual assessment, to ensure the associated risk remains at an acceptable level. This status will be assigned automatically once the Risk Acceptance has been signed by the DHS CISO.
Close Approved	Indicates that a Completed POA&M has been evidence reviewed, validated by the ISSM and remediated/mitigation has been closed.
Close Denied	Indicates that a Completed POA&M has been rejected. The reviewer has determined that the ISSM has not been provided with the appropriate evidence to validate that finding or vulnerability has been remediated/mitigated and remains “other than satisfied” as a weakness. The individual responsible (system owner, responsible system admin, and other designated personnel for the POA&M will be required to provide the appropriate evidence of completed remediation to the ISSM reviewer for validation.

3.17 POA&M Closures

OMB’s FISMA reporting guidance recommends that weaknesses should be considered “Completed” only when fully resolved. The System Owner, responsible system admin, and other designated personnel will provide evidence that the weakness has been remediated. ISSOs, who are responsible for tracking the completion of all POA&Ms, will provide the evidence documentation for final validation to the ISSM closing the POA&M. The ISSM will validate that all weakness, findings or vulnerabilities, and remediation evidence supports closure (such as follow up validation scans, manual test, or assessment). This should not be the same individual requesting closure in CSAM. This practice is to ensure separation of duties in an effort to protect against collusion. System Owners, or their designees, must validate all supporting documentation and evidence of weakness remediation in CSAM.

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. DHS OCISO expects Components to upload to CSAM an artifact that evidences both of the following:

- The remediation
- Test result and conclusions validating that the design and operating effectiveness of the remediation addressed the weakness and root cause

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. In addition, all milestones must be completed.

3.19 POA&M Cancellations

POA&M cancellation requests must be submitted by the ISSOs along with appropriate reasoning and artifacts to the Components Designated POA&M Manager for approval and processing in CSAM.

DHS CISOD expects ONLY the Component Designated POA&M Manager to approve POA&M cancellations requests, if one or more of the following conditions exists:

- The Component has mistakenly created the POA&M and submits cancellation request within 30 days of creation.
- An existing POA&M already addresses the weakness, vulnerability, or finding.
- The affected system is decommissioned.
- A duplicate POA&M with an exact control was created.
- The Components Designated POA&M Manager must document the justification for cancelling the POA&M, to include the appropriate artifact, original control, and POA&M ID within the justification of the approve request.

Note: In the event that the DHS POA&M Team identifies a cancellation request approved by a non-authorized POA&M manager not on file, the POA&M will be rolled back to its previous state. POA&M cancellations will be reviewed on an ongoing basis by the DHS POA&M Team.

3.20 Waivers

A “Waiver” status indicates that the POA&M has been granted a Waiver by the DHS CISO. Waiver requests must meet the requirements of DHS Sensitive Systems Policy Directive 4300A, Attachment B. In addition to attaching the completed waiver to the POA&M, DHS CISOD will document the following information in the POA&M:

- Waiver number and status of the waiver.
- Waiver expiration date.

A waiver does not bring the system into compliance with policy; it is an acknowledgement by the component CISO of the system’s non-compliance with policy and that an acceptable plan (within 12 months) to remediate the weakness has been provided and compensating controls have been implemented. As such the component CISO expects the component to continue to work and maintain POA&Ms with waivers.

Refer to the DHS 4300A Attachment B, "Waiver and Risk Acceptance Request" for additional guidance on the Waiver Process.

3.21 Risk Acceptance

In rare cases, if a waiver for remediation is unsuccessful, the System Owner and Component CISO can present a case for accepting the risk to the AO and DHS CISO, who may make the decision to accept the risk at their discretion because there is no viable remediation. After approval, Risk Acceptance shall be reviewed at least annually, or with every annual assessment, to ensure the risk remains acceptable and updated as events occur and information changes.

Refer to the DHS 4300A Attachment B, "Waiver and Risk Acceptance Request" for additional guidance on the Risk Acceptance Process.

4.0 CSAM POA&M PROCESS

The information that follows outlines the specific steps required to ensure that POA&Ms are developed, maintained, and closed in accordance with *Section 3 POA&M Content and Process.*

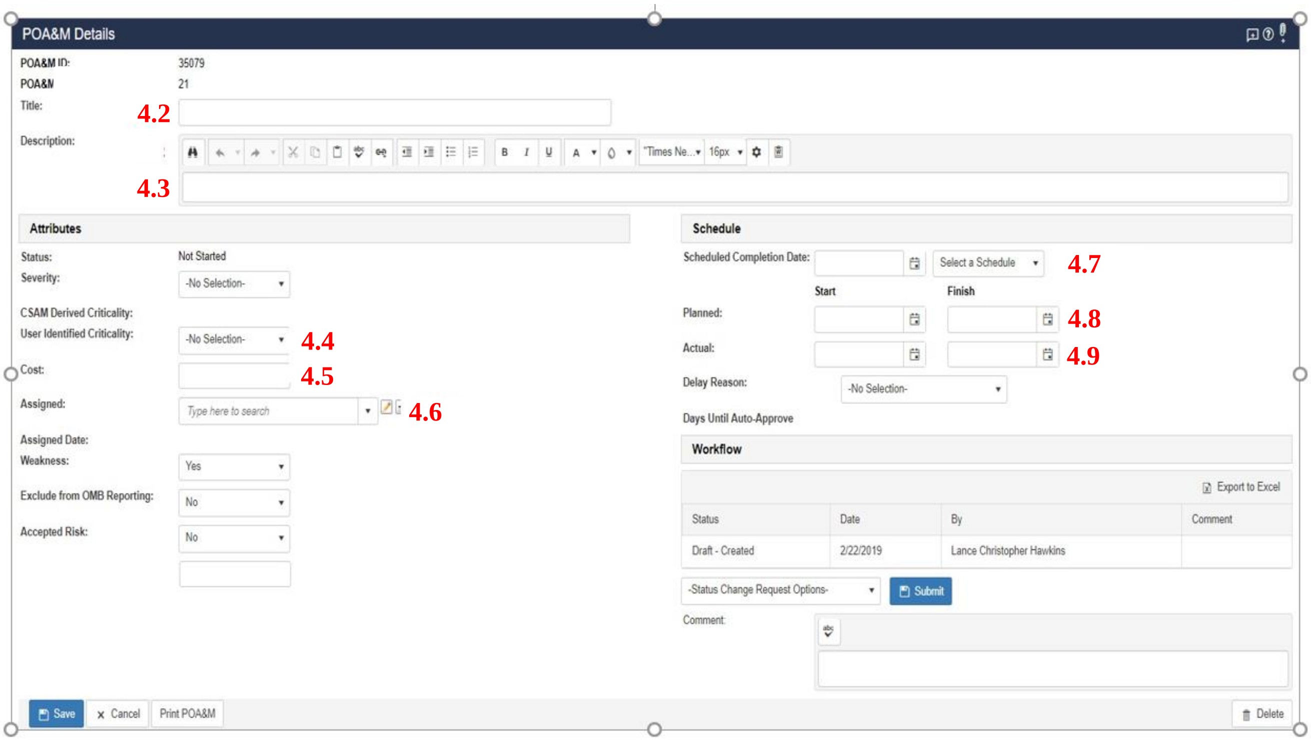
To complete these activities, you must log into the CSAM portal, https://csam.dhs.gov/CSAM/. If you have login issues, contact the DHS Infosec Help Desk for assistance.

4.1 Drafting a POA&M

You can create a new POA&M by:

- Selecting the, "Add New POA&M" button on the POA&M Listings page in your system's CSAM instance.
- On the POA&M's tab after selecting a security control from the results of a search on the Assessment Search page; or
- On the assessment results page of a control/determine if statement (DIS)[3]
- CSAM will prompt you with "Are you sure you want to create a new POA&M?" Select "Yes." A POA&M page will open in a new window.

[3] POA&M's drafted from the DIS assessment's results view will be populate with a title and description based off the security assessment finding results. You can edit the title and description as needed.



POA&M Details

POA&M ID: 35079
POA&N 21
Title:
Description:

Attributes

Status: Not Started
Severity: -No Selection-
CSAM Derived Criticality:
User Identified Criticality: -No Selection-
Cost:
Assigned: Type here to search
Assigned Date:
Weakness: Yes
Exclude from OMB Reporting: No
Accepted Risk: No

Schedule

Scheduled Completion Date: Select a Schedule
Planned:
Actual:
Delay Reason: -No Selection-
Days Until Auto-Approve

Workflow

Status	Date	By	Comment
Draft - Created	2/22/2019	Lance Christopher Hawkins	

-Status Change Request Options-
Comment:

4.2 Adding a POA&M Title

Enter the POA&M title and select save or continue to enter additional POA&M information.

4.3 Adding a Weakness Description

Enter the weakness description and select save or continue to enter additional POA&M information.

4.4 Assigning Criticality

CSAM will automatically assign a weakness criticality. If changes are necessary, click the drop-down menu and select the appropriate criticality value upon completion of a risk analysis. Once a selection has been made, select save or continue to enter additional POA&M information.

4.5 Adding the Cost

Enter the estimated costs and select save or continue to enter additional POA&M information.

4.6 Assigning the Responsible Point of Contact

In the assigned field, begin typing the responsible POC first or last name. CSAM will filter the contact list results and populate a list of contacts to select based off your entry. If the point of contact does not have information stored in CSAM, click the “Add POC” button to create a contact profile/record. In the POC profile page, populate the profile with contact information and select save. This contract profile will be available moving forward. Next, select save or continue to enter additional POA&M information.

4.7 Adding a Scheduled Completion Date

Set the scheduled completion date associated with the POA&M by manually entering the date, using the calendar pop popup, or by selecting the "Select and Schedule" button and selecting the appropriate schedule duration. Next, select save or continue to enter additional POA&M information.

4.8 Adding a Planned Start and Finish Date

Set the planned start and finish dates associated with the POA&M by manually entering the date (e.g., MM/DD/YYYY) or by using the calendar pop popup and select save or continue to enter additional POA&M information.

4.9 Adding an Actual Start and Finish Date

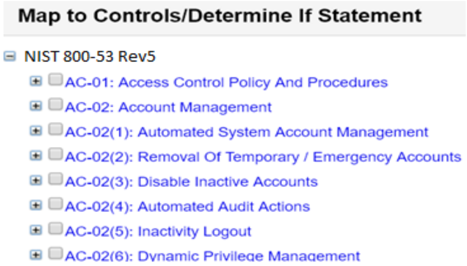
Set the actual start and finish date associated with the POA&M by manually entering the date (e.g., MM/DD/YYYY) or by using the calendar pop popup and select save or continue to enter additional POA&M information.

4.10 Associating POA&Ms with Security and Privacy Controls, Programs, and Deviations

Security and Privacy Control/Determine if Statement, programs, and deviations associated with a POA&M are located on the Associations Tab of the POA&M page.

4.11 Control/Determine If Statement

Under Control/Determine If Statement, in edit mode you have the option to select security and privacy controls and determine if statements associated with the POA&M[4].



Map to Controls/Determine If Statement

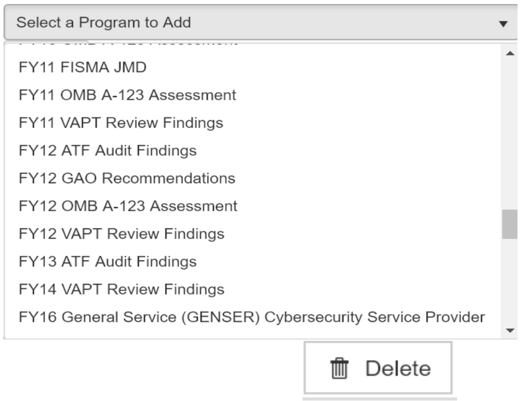
⊟ NIST 800-53 Rev5
- ⊞ □ AC-01: Access Control Policy And Procedures
- ⊞ □ AC-02: Account Management
- ⊞ □ AC-02(1): Automated System Account Management
- ⊞ □ AC-02(2): Removal Of Temporary / Emergency Accounts
- ⊞ □ AC-02(3): Disable Inactive Accounts
- ⊞ □ AC-02(4): Automated Audit Actions
- ⊞ □ AC-02(5): Inactivity Logout
- ⊞ □ AC-02(6): Dynamic Privilege Management

Upon completion of this activity, select save.

4.12 Programs

Under Programs, in edit mode you have the option to select a program to associate with the POA&M. Select the appropriate program, select "Add" and the selected program will populate the Program Name record list.

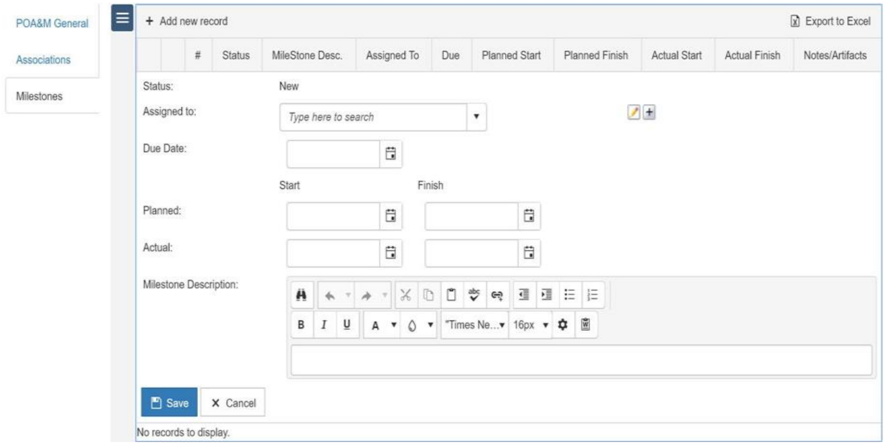
[4] During security control assessment activities, you can link security controls and determine if statements to existing POA&Ms. When this occurs, those additional links will display in this view.


Select a Program to Add
FY11 FISMA JMD
FY11 OMB A-123 Assessment
FY11 VAPT Review Findings
FY12 ATF Audit Findings
FY12 GAO Recommendations
FY12 OMB A-123 Assessment
FY12 VAPT Review Findings
FY13 ATF Audit Findings
FY14 VAPT Review Findings
FY16 General Service (GENSER) Cybersecurity Service Provider
Delete

If you accidentally add the wrong program, select “Delete” and it will remove the entry from the Program Name record list.

4.13 Adding Milestones

Milestones associated with a POA&M are located on the milestones tab of the POA&M page. To add a milestone, select, “Add New Record” and enter milestone information. Follow the procedures below to complete this activity.



Status: New

Assigned to: Type here to search

Due Date:

Planned:

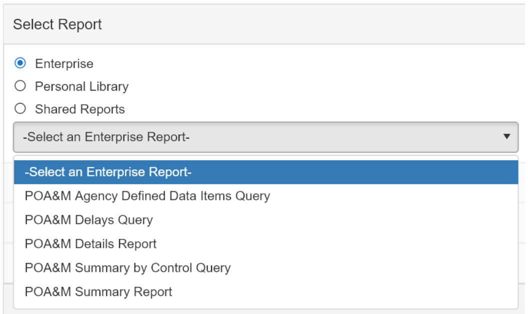
Actual:

Milestone Description:

No records to display.

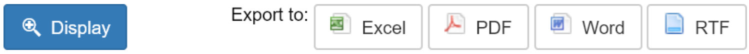
4.14 Generating a POA&M Summary Report

To generate a POA&M summary report, click on the system’s CSAM instance under the POA&M Reports/View tab.


Select Report
● Enterprise
○ Personal Library
○ Shared Reports
-Select an Enterprise Report-
-Select an Enterprise Report-
POA&M Agency Defined Data Items Query
POA&M Delays Query
POA&M Details Report
POA&M Summary by Control Query
POA&M Summary Report

Once you select POA&M Summary Report, you can then search for specific POA&M information parameters under the filters tab as well as select the output columns to be populate under the output columns tab in order to generate a tailored report.

Once you have selected the customizable options, you can select one of the following output options to generate the report: “Excel, PDF, Word, or RTF”. The “Display” option will generate a report that is viewable in the CSAM application whereas the other four (4) options are programs where the report can be exported.



5.0 QUESTIONS

Comments concerning the DHS Information Technology Security Program, Sensitive Systems, Attachment H – DHS POA&M Guide are welcomed and should be submitted to DHS CISOD (canda@hq.dhs.gov).