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.

		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.*

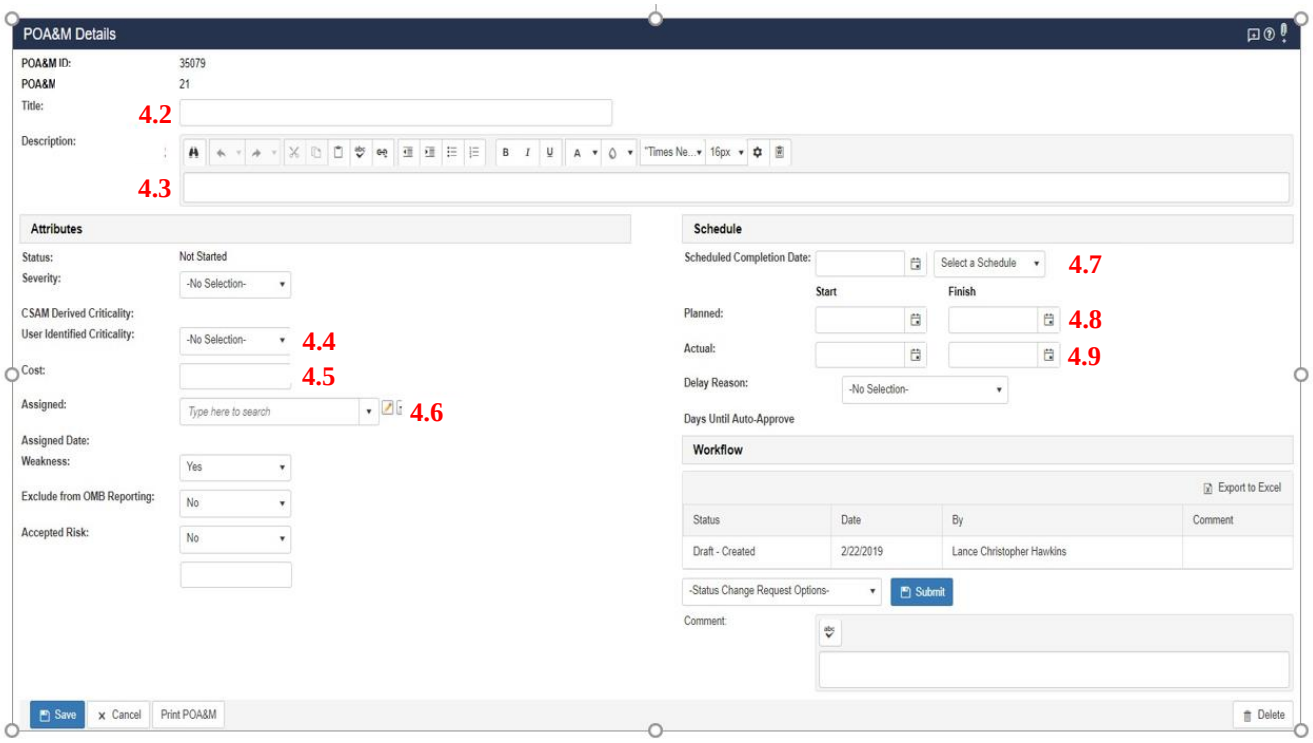
To complete these activities, you must log into the CSAM portal, https://csam.dhs.gov/CSAM/. If you have login issues, contact the DHS Infosec Help Desk for assistance.

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.



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

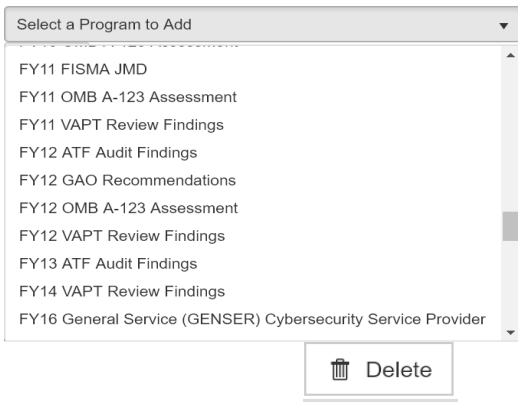
Under Control/Determine If Statement, in edit mode you have the option to select security and privacy controls and determine if statements associated with the POA&M[4].

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.

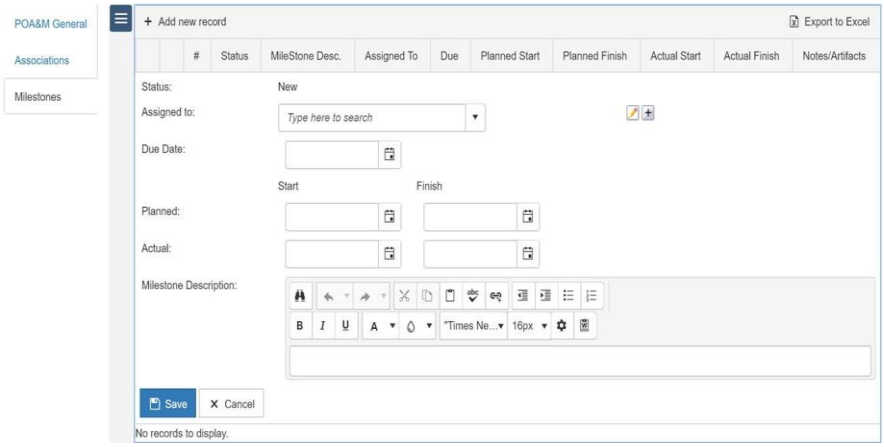
[4] During security control assessment activities, you can link security controls and determine if statements to existing POA&Ms. When this occurs, those additional links will display in this view.



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

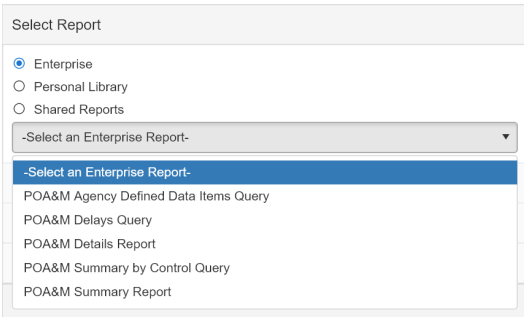
4.13 Adding Milestones

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.



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.



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).