NOAA Cybersecurity Standard:

POA&M Management Process

Version 1.0
June 25, 2019
Change / Revision Record

This standard is reviewed and updated on an annual basis and as often as needed to ensure accuracy of information. It is effective until cancelled by the NOAA Cyber Security Director or designee. OCIO, CSD will maintain this document to ensure it is up-to-date, and will summarize modifications (if any) to this document in the table below. This record will be maintained throughout the life of the document.

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description of Change/Revision</th>
<th>Section / Pages Affected</th>
<th>Changes Made by Name / Title / Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>5/13/2019</td>
<td>Initial draft</td>
<td>All</td>
<td>NWS ITSO (content)</td>
</tr>
<tr>
<td>0.2</td>
<td>5/23/2019</td>
<td>Added change to role allowing ITSO to delegate POA&amp;M closure approval.</td>
<td>Various</td>
<td>M. Noto, OCIO, CSD</td>
</tr>
<tr>
<td>1.0</td>
<td>6/25/2019</td>
<td>Finalized draft</td>
<td>All</td>
<td>M. Noto, OCIO, CSD, S. Lutsky, OCIO, CSD</td>
</tr>
</tbody>
</table>
Document Approval

JONES.JAMES.I
V.1049453465
Digitally signed by
JONES.JAMES.IV.1049453465
Date: 2019.07.03 12:53:58
-04'00'

Director, Cyber Security Division

Document Review

ROGERS.WILLIAM.GUY.15207
68811
Digitally signed by
ROGERS.WILLIAM.GUY.1
520768811
Date: 2019.07.02
11:10:54 -04'00'

NOAA IT Security Officer (ITSO)
### Contents

**Introduction**  
- Background  
- Purpose  
- Scope  
- Assumptions  
- References  

**Roles & Responsibilities**  
- 2.1 Information System Owner (ISO or SO)  
- 2.2 Information System Security Officer (ISSO)  
- 2.3 Cyber Security Program Manager (CSPM)/Information Technology Security Officer (ITSO)  

**Process**  
- 3.1 Creation Requirements  
- 3.2 Draft Approval  
- 3.3 POA&M Closure  
- 3.4 POA&M Cancellation  
- 3.5 Delayed POA&Ms  

**4. Compliance/Verification**  

**5. Non-Compliance**  

**Appendix A – POA&M Elements**  

**Appendix B – POA&M Creation Procedures in CSAM**  

**Appendix C – Draft Approval Request in CSAM**  

**Appendix D – Closure or Cancellation Request in CSAM**
1. Introduction

In Accordance with the Federal Information System Modernization Act (FISMA) of 2014, a Plan of Action and Milestones (POA&M) serves as a corrective action plan for tracking and planning the resolution of information system security weaknesses within government agencies. The NOAA POA&M Management Process document is a standard for creating and managing POA&Ms to remediate information security weakness in NOAA information systems.

1.1 Background

The Office of Management and Budget (OMB) requires agencies to develop, implement, and manage POA&Ms for all programs and systems they operate and control. POA&Ms identify and track system-specific vulnerabilities across the NOAA Enterprise. All NOAA FISMA systems must utilize the DOC mandated Cyber Security Assessment and Management (CSAM) tool for the POA&M management process. NOAA requires that every information system update POA&Ms to reflect the current progress against planned remediation efforts.

1.2 Purpose

The purpose of this document is to provide guidance to NOAA information systems to properly manage and rectify system level weaknesses or flaws. This document also complies with Department of Commerce (DOC) POA&M Minimum Standards.

1.3 Scope

This process applies to all NOAA information systems where system specific weaknesses have been identified and a POA&M needs to be created.

1.4 Assumptions

CSAM access and basic operation knowledge are assumed by those leveraging this document. For detailed instructions on how to operate CSAM, please refer to the latest CSAM User Guide available on https://max.gov. In addition, CSAM Q&A sessions are facilitated every 3rd Thursday of the month. For more information on these sessions please visit the Max.gov portal.

1.5 References

- Department of Commerce, POA&M Minimum Standards, July 31, 2017
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Rev.2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev.4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
2. Roles & Responsibilities

2.1 Information System Owner (ISO or SO)

Per NOAA IT Security Manual 212-1301 version 6.0, ISOs/SOs ensure all applicable controls are effective and operating as intended, and for those with POA&Ms, ensure actions are taken and POA&Ms are closed on schedule.

2.2 Information System Security Officer (ISSO)

ISSOs develop, track, and manage POA&Ms for their specific systems.

2.3 Cyber Security Program Manager (CSPM)/Information Technology Security Officer (ITSO)

Per NOAA IT Security Manual 212-1301 version 6.0, CSPMs/ITSOs develop and track entity level remedial actions to mitigate risks in accordance with DOC policies and procedures. The LO CSPM/ITSO may delegate POA&M review & closure for Low and Moderate Impact systems and moderate risks for High Impact systems to the ISO/SO.

3. Process

Each POA&M undergoes several stages. A POA&M is created after a weakness is identified during any of the following: Office of Inspector General (OIG) audits, the annual Security Control Assessment (SCA), or other internal audits requiring a corrective action plan. POA&Ms are developed by the ISSO or designated system personnel, undergo review by the Compliance Team, and then are approved by the responsible CSPM/ITSO. Once development and review have been completed, the POA&M is managed and tracked until completion. The NOAA POA&M process begins with system personnel developing a remediation plan, which should be completed within a reasonable period (scheduled completion date). The process includes:

- Determining (with stakeholder involvement) the root cause of the vulnerability/IT weakness, cost of remediation, and who should be involved in resolving the weakness.
- Determining the severity level of weakness in order to prioritize POA&M efforts according to risk factors.
- Developing a timeline for remediation by defining activities that are clear, logical, and measurable, with a reasonable completion date.
- Assigning responsibility for remediation and developing internal controls to monitor and update the POA&M to demonstrate weekly to monthly progress.
- Monitoring vulnerability/weakness to prevent delays in scheduled completion dates.

The workflow below encapsulates the NOAA POA&M Management process.
POA&M Management Workflow

Figure 1: POA&M Management Workflow
3.1 Creation Requirements

a. All vulnerability/weaknesses must be tracked/created in CSAM prior to the ATO brief and presented to the Authorizing Official (AO) for their review as part of the Risk Management Process.

b. Weaknesses remediated after the onsite assessment require a POA&M for tracking purposes.

c. Identified weaknesses determined by system personnel to be an acceptable risk are required to be tracked in a POA&M. The accepted risk is to be formally documented within the approved FIPS 200 control-tailoring document. A risk acceptance form must be completed as an appendix to the FIPS 200. AO’s must be briefed on the proposed accepted risks and risks must be approved prior to documentation.

d. Similar findings (i.e., findings such as multiple identical vulnerabilities at the same criticality level on devices of a similar class and OS, NOT all results of a vulnerability scan across a network/subnet) may be consolidated under one POA&M to remediate the primary risk.

e. All POA&Ms must be mapped to applicable controls and documented in CSAM.

f. Scheduled completion date for each weakness must be based on realistic timelines that allow for resources to be obtained and the associated steps to be completed. System personnel should also consider contingencies (e.g., critical weather days, procurement delays; etc.). Every effort must be taken to ensure all POA&Ms are closed prior to the next Assessment & Authorization (A&A).

g. POA&M scheduled completion dates shall not be changed once entered into CSAM. However, dates may be adjusted for milestones with written concurrence from the system owner.

h. Identified cost associated with a POA&Ms value cannot be $0 or $1. Please refer to Department of Homeland Security Process Guide for Plan of Action and Milestones (Appendix H9) as a reference for minimum cost estimates for remediating system weaknesses.

i. All POA&Ms related to a system being decommissioned must be closed and validated prior to decommissioning.
3.2 Draft Approval

a. “Draft Created” must be used for inputting POA&Ms that are a result of the ATO process prior to the issuance of the ATO. Once the ATO is granted, the ISSO must update any outstanding elements or milestones and advance the POA&M to “Draft Approval Request Status”. All POA&Ms must be advanced to “Draft Approval Request” within ten (10) business days of attaining ATO.

b. The relevant authorizing official’s designated representative (AODR)/ITSO/certification agent or other designated position will review POA&Ms to determine all elements and appropriate milestones are included. If there are missing elements, the compliance/review team will contact the ISSO and request that the missing elements be provided.

c. All POA&Ms entered into CSAM will be reviewed against the A&A Package to ensure all elements are included before approval.

d. ISO/SOs and ISSOs are responsible for managing POA&Ms in CSAM.

e. All POA&Ms must have milestones including a milestone to review and must update the System Security Plan (SSP) or other key documentation if applicable; all fields relevant to POA&M mitigation must be completed for a POA&M to be approved.

f. Appendix C “Draft Approval Request in CSAM” provides guidance for draft approval.

3.3 POA&M Closure

a. POA&Ms submitted for closure will be reviewed by the relevant LO/OCIO ITSO (or delegate, e.g., SO), and closure will be granted if all the required components are in place.

b. Artifacts that validate the mitigation of system-level weakness must be uploaded when submitting a POA&M for closure. When possible, please attach artifacts to the corresponding milestone for final submissions.

c. See Appendix D “Closure or Cancellation Request in CSAM” for additional closure request guidance.

3.4 POA&M Cancellation

a. POA&M cancellation requests will be reviewed on a case-by-case basis and approval shall be granted by the Authorizing Official.

b. For all POA&M cancellation request, artifacts and/or explicit rationale must be provided to support the request.

c. Appendix D “Closure or Cancellation Request in CSAM” provides guidance for
cancellation requests.

3.5 Delayed POA&Ms

a. The relevant authorizing official’s designated representative (AODR)/ITSO/certification agent or other designated position will contact system personnel regarding POA&Ms coming due within 30, 60, 90 days.

b. A month prior to a POA&M going delayed, the relevant authorizing official’s designated representative (AODR)/ITSO/certification agent or other designated position will contact system personnel on a more frequent basis for status updates.

c. In the event there are anticipated delays, the system personnel must contact the relevant ITSO, System Owner, and Authorizing Official to brief them on the status of remediation plans and the suggested course of action moving forward.

d. To prevent delays, it is recommended to submit POA&Ms for closure at the minimum ten (10) business days prior to scheduled completion date to allow for review and approval from the relevant authorizing official’s designated representative (AODR)/ITSO/certification agent or other designated position.

e. Upon determination of a POA&M delay, the ISO or ISSO will provide the relevant ITSO, System Owner, and Authorizing Official justification for the delay, which should be entered in CSAM in the delayed justification section.

f. Once a POA&M becomes delayed, the relevant authorizing official’s designated representative (AODR)/ITSO/certification agent or other designated position will provide frequent reminders to system personnel.

g. Additionally, when a POA&M becomes delayed, the relevant authorizing official’s designated representative (AODR)/ITSO/certification agent or other designated position will provide frequent notifications to the Authorizing Official.

h. In the event a POA&M goes delayed without any justification or communication with the ITSO, the ITSO will escalate to the Authorizing Official for a resolution.

i. When a POA&M goes delayed, the ITSO will escalate to the Authorizing Official for a resolution.

4. Compliance/Verification
To ensure compliance with the POA&M management process, NOAA ITSOs and the NOAA OCIO compliance team will perform quality reviews via CSAM. Verification information for each step in the process is located in Section 3.

5. Non-Compliance

Compliance with this NOAA POA&M management process is mandatory. Non-compliance will be reported to the LO/SO ITSO, the NOAA ITSO, and other management officials. Further action may be taken as a result of non-compliance.
Appendix A – POA&M Elements

a. **POA&M Title**: A short relevant title that includes a description of the deficiency. This must be captured from the SAR or ATO Briefing Slide.

b. **POA&M ID**: Automatically generated by CSAM at POA&M creation that cannot be updated by the user or reused.

c. **POA&M Sequence**: Automatically assigned by CSAM when the POA&M is created.

d. **Weakness Description**: Include weakness description from the Security Assessment Report (SAR) or other source. Additional concise information to accurately identify vulnerability can be added.

e. **User Identified Criticality**: Identify criticality of POA&M-refer to recommended risk level identified in the SAR or source.

f. **POA&M Scheduled Completion Date**: Date POA&M will be completed. Do not use TBD; dates must be realistic and achievable.

g. **Cost**: Provide a best estimated cost for resolving the issue. Typically this will be labor hours and materials, service costs, etc.

h. **Assigned**: The responsibility for remediation must be assigned to system personnel who can assist in mitigation.

i. **Associations**: Controls related to a vulnerability must be mapped to each POA&M.

j. **Actionable Milestones**: The actions to be taken to resolve the identified issue. Every POA&M must have milestones that communicate key achievements to be reached towards remediation.

k. **Milestone Assigned**: System personnel assigned to assist in steps needed to resolve identified weakness.

l. **Milestones with Planned Start/Finish Dates**: The expected start and finish dates.

m. **Planned Finish Date**: The expected finish date.
Appendix B – POA&M Creation Procedures in CSAM

1. Select the Management/Overview tab on the CSAM homepage, select “POA&Ms”, and then select “Add POA&M”.

2. Select the System tab and “Search Systems” from the automatic drop down menu on the CSAM Dashboard page.

On the following page, search for a system using the provided filters.

\[\text{The following figures were captured from the DOC Plan of Action and Milestones Minimum Standards, July 2017.}\]
After the correct system is returned, click “Details” to access the system’s page.

Select “POA&M Listing” from the menu on the left hand side of the page.
Select “Add New POA&M” next to the “Search By POA&M ID” bar, as shown in the following image.

**Figure B-7 Add New POA&M bar**

**POA&M ID:** Automatically generated ID established at POA&M creation that cannot be updated by the user or reused within the application. This ID increases each time a POA&M is established for any system in CSAM.

**POA&M Seq:** The POA&M sequence number for the POA&M in question. This number cannot be changed by the user and is automatically assigned by CSAM when the POA&M is created.

**Create Date:** The CSAM generated creation date for the POA&M in question.

**Title:** The user identified title for the POA&M in question. The title must contain: a brief description of the finding.

**Description:** The complete description of the POA&M.
<table>
<thead>
<tr>
<th>Attributes</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not Started</td>
</tr>
<tr>
<td>Severity</td>
<td>-No Selection-</td>
</tr>
<tr>
<td>CSAM Derived Criticality</td>
<td></td>
</tr>
<tr>
<td>User Identified Criticality</td>
<td>-No Selection-</td>
</tr>
<tr>
<td>Cost</td>
<td>$0</td>
</tr>
<tr>
<td>Assigned</td>
<td></td>
</tr>
<tr>
<td>Assigned Date</td>
<td></td>
</tr>
<tr>
<td>Weakness</td>
<td>Yes</td>
</tr>
<tr>
<td>Exclude from OMB Reporting</td>
<td>No</td>
</tr>
<tr>
<td>Accepted Risk</td>
<td>No</td>
</tr>
<tr>
<td>GAO Audit</td>
<td>No</td>
</tr>
<tr>
<td>OIG Audit</td>
<td>No</td>
</tr>
<tr>
<td>FISMA Audit</td>
<td>No</td>
</tr>
<tr>
<td>Financial Statements Audit</td>
<td>No</td>
</tr>
</tbody>
</table>
Status: The current status of the POA&M. The user should select from the dropdown menu consisting of the following options below:

- **Not Started**: POA&M is still in Draft Status and has not been approved.
- **Planned/Pending**: POA&M is Approved with a required Scheduled Completion Date and Planned Start/Finish Dates.
- **In Progress**: POA&M is approved with a Scheduled Completion Date, Planned Start/Finish Dates, and an Actual Start Date.
- **Delayed (Late)**: POA&M is Approved and passed the Scheduled Completion Date.
- **Cancelled**: POA&M has been requested and approved to be cancelled.
- **Completed**: POA&M has been closed and completed.

User Identified Criticality: The user identified risk associated with this POA&M. The user must select one of the following risk levels from the dropdown menu:

- **Very Low**
- **Low**
- **Medium**
- **High**
- **Very High**

Cost: The user identified cost associated with this POA&M. This value cannot be $0 or $1.

Assigned: The user identified CSAM point of contact assigned to this POA&M. A POA&M can only be assigned to one individual at a time (usually the ISSO).

Weakness: Field to identify if a POA&M is a weakness to the system(s) or not.

**Schedule**

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Completion Date</td>
<td><img src="(select_a_schedule.png)" alt="Select a Schedule" /></td>
</tr>
<tr>
<td>Planned Start</td>
<td><img src="start.png" alt="Start" /></td>
</tr>
<tr>
<td>Planned Finish</td>
<td><img src="finish.png" alt="Finish" /></td>
</tr>
<tr>
<td>Actual Start</td>
<td><img src="actual_start.png" alt="Actual Start" /></td>
</tr>
<tr>
<td>Actual Finish</td>
<td><img src="actual_finish.png" alt="Actual Finish" /></td>
</tr>
<tr>
<td>Delay Reason</td>
<td><img src="no_selection.png" alt="No Selection" /></td>
</tr>
</tbody>
</table>

**Scheduled Completion Date**: Original due date of the POA&M. It must be entered in MM/DD/YYYY format or selected in calendar. This date cannot be changed after it is submitted.
Planned Start:  Planned start date for implementation of the POA&M. It must be entered in MM/DD/YYYY format or selected in calendar.

Planned Finish:  Planned finish date for implementation of the POA&M. In lieu of updating the Due Date, the user should use the planned finish date to update the scheduled completion date for the POA&M. It must be entered in MM/DD/YYYY format or selected in calendar.

Actual Start:  Actual start date for implementation. It must be entered in MM/DD/YYYY format or selected in calendar.

Actual Finish:  Actual finish date for implementation. It must be entered in MM/DD/YYYY format or selected in calendar.

Delay Reason:  A drop down list from which the user can select the reason a POA&M is delayed, if the POA&M has proceeded past the Due Date prior to completion.
Association: Field to identify controls related to a POA&M.

Milestones: The actions to be taken to resolve the identified issue for each POA&M.
Appendix C – Draft Approval Request in CSAM

1. Select the Edit tab on the POA&M details page, as shown in the following image.

![POA&M Details Section in CSAM](image)

---

**Figure C-1 POA&M Details Section in CSAM**
2. Select the Status Change Request Options tab and click on “Draft – Approval request” option from the drop down menu and click Submit.

Figure C-2 POA&M Details Section in CSAM
3. After submitting “Draft Approval Requested”, click Save.

![Figure C-3 POA&M Details Section in CSAM](image-url)
Appendix D – Closure or Cancellation Request in CSAM

1. Select the Edit tab on the POA&M details page, as shown in the following image.

![Figure D-1 POA&M Details Section in CSAM](image-url)
2. Select the Status Change Request Options tab and click on the “POA&M Close Requested” or “POA&M Cancellation Requested” option from the drop down menu and click Submit.

![Figure D-2 POA&M Details Section in CSAM](image)

3. After submitting the “POA&M Close Requested” or “POA&M Cancellation Requested” option, click Save.
Figure D-3 POA&M Details Section in CSAM