

# NESDIS

## Plan of Action and Milestones (POA&M) Management Policy and Procedures

**September 28, 2012**



**Prepared by:**

**U.S. Department of Commerce  
National Oceanic and Atmospheric Administration (NOAA)  
National Environmental Satellite, Data, and Information Service (NESDIS)**

## Table of Contents

NESDIS Plans of Action and Milestones (POA&M) Management Policies and Procedures .....	6
1.0 Background and Purpose .....	7
2.0 Scope .....	7
3.1 Roles, Responsibilities, and Coordination.....	7
3.2 Authorizing Official (AO).....	7
3.3 System Owner (SO).....	7
3.4 Information System Security Officer (ISSO).....	8
3.5 Information Technology Security Officer (ITSO) .....	8
4.0 Management Commitment .....	8
5.1 Compliance.....	8
5.2 References.....	8
6.1 NESDIS POA&M Management Policy .....	10
6.2 Policy Maintenance .....	10
6.3 Policy Feedback Process .....	10
6.4 Policy Effective Date .....	10
7.1 Procedures .....	10
7.2 POA&M Identification .....	10
7.3 Risk Acceptance.....	13
7.4 POA&M Initiation .....	16
7.3.1 Low and Moderate Risk Weaknesses .....	16
7.3.2 High Risk Weaknesses .....	18
7.3.3 Add POA&M in CSAM .....	23
7.3.4 Update POA&M in CSAM .....	23
7.3.4.1 POA&M Search.....	23
7.3.4.2 POA&M General Tab .....	25
7.3.4.3 Source.....	27
7.3.4.4 Cost Comments .....	28
7.3.4.5 Adding a Point of Contact in CSAM .....	28

7.3.4.6	Security Control Mapping.....	30
7.3.4.7	POA&M Milestones Tab .....	30
7.3.5	Update Status .....	32
7.3.6	Remove or Cancel a POA&M.....	32
7.3.6.1	Remove a POA&M.....	32
7.3.6.2	Cancel a POA&M .....	34
7.3.7	Sensitive Information .....	34
7.3.8	Scheduled Completion .....	35
7.3.9	Consolidated Reporting.....	35
7.3.10	Identify POA&Ms for Review.....	38
7.4	POA&M Management .....	38
7.4.1.	Tracking Tools.....	40
7.4.1.1	CSAM Start Page.....	40
7.4.1.2	POA&M Search Form.....	40
7.4.1.3	POA&M Reports .....	40
7.4.1.4	Tasks.....	41
7.5	POA&M Completion .....	41
7.5.1	Low to Moderate Risk Weaknesses.....	41
7.5.2	High Risk Weaknesses .....	43
7.5.3	Closure Request Review .....	45
7.5.4	Report Closure.....	47
7.5.5	Artifacts and Supporting Files.....	47
7.5.5.1	File Types.....	47
7.5.5.2	Shared Artifacts or Files.....	48
7.5.5.3	Upload an Artifact .....	51
7.5.6	Identify Closed POA&Ms for Review .....	52
7.5.6.1	Perform a review .....	52
7.6	CSAM Workflow and Approval Status .....	53
7.7	POA&M Review Checklist.....	56



UNITED STATES DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration  
NATIONAL ENVIRONMENTAL SATELLITE  
DATA AND INFORMATION SERVICE  
Silver Spring, Maryland 20910

September 30, 2012

**MEMORANDUM**

Distribution

**FOR: FROM:**

Catrina D. Purvis   
NESDIS Chief Information Officer (Acting)

**SUBJECT:**

Issuance of Updated NESDIS Information  
Technology Security Policies and Procedures

This is to announce the issuance of ten updated NESDIS publications for implementing effective, compliant, and consistent information technology (IT) security practices within NESDIS. These documents highlight the specific steps necessary to ensure effective NESDIS implementation. Specifically issued under this memorandum are the

1. NESDIS *Federal Information Processing Standard 199 Security Categorization Policy and Procedures*, v3.0;
2. NESDIS *Plan of Action and Milestones Management Policy and Procedures*, v2.0;
3. NESDIS *Policy and Procedures for Determining Minimum Documentation Requirements for System/Interconnections*, v2.1;
4. NESDIS *Contingency Planning Policy and Procedures*, v2.1;
5. NESDIS *Policy and Procedures for Ensuring Security in NESDIS IT Systems and Services Acquisitions*, v2.1;
6. NESDIS *Security Assessment Report Policy and Procedures*, v2.0;
7. NESDIS *Federal Information Security Management Act (FISMA) Inventory Management Policy and Procedures*, v2.0;
8. NESDIS *IT Security Training Policy and Procedures*, v2.1;
9. NESDIS *Continuous Monitoring Planning Policy and Procedures*, v2.1; and the
10. *Practices for Securing Open-source Project for a Network Data Access Protocol Server Software on NESDIS Information Systems*, v3.1.

These publications are part of the NESDIS-wide effort to maintain and enhance its foundation of NESDIS IT security policies and implementation practices that align with the latest Department of Commerce and NOAA policies, requirements, and standards. I wish to thank all who contributed reviewing and commenting on the drafts prior to publication to ensure

that they are complete, current, and meaningful. These documents will be posted to the Chief Information Division's Web site at [https://intranet.nesdis.noaa.gov/ocio/it\\_security/handbook/itsecurityhandbook.php](https://intranet.nesdis.noaa.gov/ocio/it_security/handbook/itsecurityhandbook.php). If you have any questions, please contact the NESDIS IT Security Officer, Nancy DeFrancesco, at [Nancy.DeFrancesco@noaa.gov](mailto:Nancy.DeFrancesco@noaa.gov) or phone (301) 713-1312.

## NESDIS Plans of Action and Milestones (POA&M) Management Policies and Procedures

### Record of Changes/Revisions

Version	Date	Section	Author	Change Description
Final 1.0	8/31/2009	3.0, 3.4, 3.5, 7.1, 7.2, 7.3, 7.5, Table 4	N.DeFrancesco	Address comments on final draft and finalize for issuance by CIO.
1.1	9/14/2009	All	N.DeFrancesco	Correct numbering and formatting errors in document conversion.
1.2d	2/9/2012	All	A.Kuhn	Annual Update
2.0f	09/28/2012	All	N.DeFrancesco	Finalize and prepare for CIO issuance

## **1.0 Background and Purpose**

The Federal Information Security Management Act requires that agencies establish “...a process for planning, implementing, evaluation, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.” The Plan of Action and Milestones (POA&M) implements this requirement and is used to track corrective actions for deficiencies in an Information Technology (IT) security program or system security control. The Office of Management and Budget annually issues reporting requirements for the development of POA&Ms and has established formats for POA&Ms, as well as performance metrics.

Appendix E of the Department of Commerce (DOC) *Information Technology Security Program Policy* (ITSPP) establishes the DOC policy for development and management of POA&Ms. DOC uses the Cyber Security Assessment and Management (CSAM) tool to record and manage POA&Ms across the Department. CSAM provides DOC an enterprise-wide view of security for all systems.

This document communicates NESDIS-specific POA&M management policy and describes procedures for implementing the POA&M requirements within NESDIS including use of CSAM for creating, managing, and closing POA&Ms. It is a companion document to the *NESDIS Risk Management Framework Assessment & Authorization Process Policy and Procedures*.

## **2.0 Scope**

The scope of this document is limited to providing NESDIS-specific policies and procedures for managing POA&Ms. It establishes responsibilities and provides step-by-step procedures for how each NESDIS Authorizing Official (AO), System Owner (SO), Information System Security Officer (ISSO), and Information Technology Security Officer (ITSO) must use CSAM to manage POA&Ms.

## **3.1 Roles, Responsibilities, and Coordination**

The policies and procedures provided in this document apply to NESDIS personnel assigned to specific roles within NESDIS. Following is a list of those roles, along with a description of high level POA&M management and coordination responsibilities for each.

### **3.2 Authorizing Official (AO)**

The AO’s primary POA&M management responsibility is to make fully informed risk acceptance determinations and approve all POA&Ms.

### **3.3 System Owner (SO)**

The SO is responsible for ensuring effective POA&M management in all stages of development from identification, initiation, management (tracking and reporting), through completion.

### **3.4 Information System Security Officer (ISSO)**

The SO may require the ISSO to provide or oversee support activities for any of the SO's POA&M management responsibilities.

### **3.5 Information Technology Security Officer (ITSO)**

The ITSO performs oversight of and ensures compliance with the NESDIS POA&M management policies and CSAM procedures established by this document. The ITSO and direct support staff oversee all stages of POA&M process, from identification, initiation, and management (tracking and reporting), through completion.

## **4.0 Management Commitment**

The NESDIS Chief Information Division (CID) supports the NESDIS Assistant Administrator's (AA) strong emphasis on securing NESDIS information and information systems. Through the issuance of these policy and procedures, the CID demonstrates its commitment to establishing a foundation for managing IT security weaknesses and corrective actions in a consistent and cost-effective manner.

## **5.1 Compliance**

The NESDIS ITSO monitors – through periodic quality reviews and monthly performance metrics – management of POA&Ms within NESDIS to ensure compliance with applicable laws, directives, policies, and guidance. The ITSO reports monthly to the AA, and to the Chief Information Officer (CIO) and Office Directors as necessary, but at least monthly, regarding compliance. The AA, CIO, and/or Office Directors may initiate actions as necessary to correct reported deficiencies, including reallocation of resources to improve implementation of security practices, or removal of an individual from their role as AO, SO, ITSO, or ISSO.

## **5.2 References**

- DOC *Information Technology Security Program Policy* ITSP section 4.4 (January 2009)
- Commerce Information Technology Requirement 018, *IT Security Plans of Action and Milestones (POA&Ms)*, (March 2012)
- NOAA *Plan of Action and Milestones (POA&M) Management Standard*, v3.0,



NESDIS Quality Procedure [NQP] – 3409  
Revision 2.1

Effective Date: September 28, 2012  
Expiration Date: Until Superseded

February 2012

## **6.1 NESDIS POA&M Management Policy**

As required by DOC ITSPP section 4.4.5, NESDIS SOs shall develop and update monthly, POA&Ms for the information system that documents the planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. The NESDIS ITSO shall monitor POA&M management by SOs and report status at least monthly to the NESDIS AAs and Office Directors.

## **6.2 Policy Maintenance**

The NESDIS ITSO shall review these policy and procedures bi-annually and update as necessary to reflect implementation challenges and new requirements. All updates to this policy shall be subject to a NESDIS-wide vetting process providing an opportunity for stakeholders to comment on the programmatic implications of updates.

## **6.3 Policy Feedback Process**

NESDIS personnel are encouraged to notify the ITSO via e-mail at [nesdis.it.security@noaa.gov](mailto:nesdis.it.security@noaa.gov) regarding any errors found in the document or other clarifications or updates that are required.

## **6.4 Policy Effective Date**

This policy is effective within 30 days of issuance.

## **7.1 Procedures**

A POA&M undergoes several phases. A POA&M is created after a weakness is identified in a source report. The POA&M is further developed and undergoes review. Once development and review have been completed, the POA&M is managed and tracked until it reaches completion.

## **7.2 POA&M Identification**

The NESDIS POA&M management process is strictly for identifying and tracking corrective actions directly related to resolving security weaknesses. The POA&M must describe the security weakness, identify its origin, the high-level corrective action plan and milestones, the schedule for completion, and the resources/individuals allocated or assigned to correct the weakness.

It is inappropriate to use the POA&M management process to schedule recurring routine IT system maintenance or IT security planning activities (e.g., routine patch

management activities, continuous monitoring security controls testing, quarterly vulnerability scans, System Security Plan (SSP) updates, etc.). Where a security

weakness has been identified for failure to complete a required recurring or routine activity (e.g., quarterly vulnerability scans), the resulting POA&M should identify the corrective action needed to ensure that the recurring routine activity is performed as required (e.g., remedial training, system re-configuration for appropriate privileges etc.), rather than a POA&M that merely schedules completion of the missed recurring or routine activity.

Consistent with DOC policy, NESDIS considers the findings of any audit or security assessment report as appropriate program and system security control Weakness Source Reports (WSR) to be used as source input requirements for POA&M Identification including, but not limited to the following:

- Office of Inspector General (OIG) audit and evaluation reports
- Government Accountability Office (GAO) audit reports
- Vulnerability Assessment Reports from quarterly system scanning
- Penetration Testing Reports
- Continuous monitoring assessment reports
- Assessment & Authorization (A&A) Security Assessment Reports (SARs)

POA&M identification procedure steps and responsibilities are as follows:

Steps 1-3 must be completed within 45 days from receipt of the WSR(s).

**Step 1.** The SO in coordination with the ISSO will perform a comprehensive WSR review:

- a. Determine the level of risk presented by each identified weakness (if not specified by the WSR). See the *NESDIS Risk Assessment Policies and Procedures* for additional guidance on how to assess levels of risk.
- b. Identify the optimal solution and corrective action(s) (if not specified by the source report).
- c. Determine the resources required.
- d. Determine resource availability.
- e. Prioritize the weakness.

f. Determine estimated completion date. See section 7.3.8 for expected mitigation of scan-related vulnerabilities and high-risk weaknesses from other sources.

g. Identify candidates for risk acceptance by AO(s).

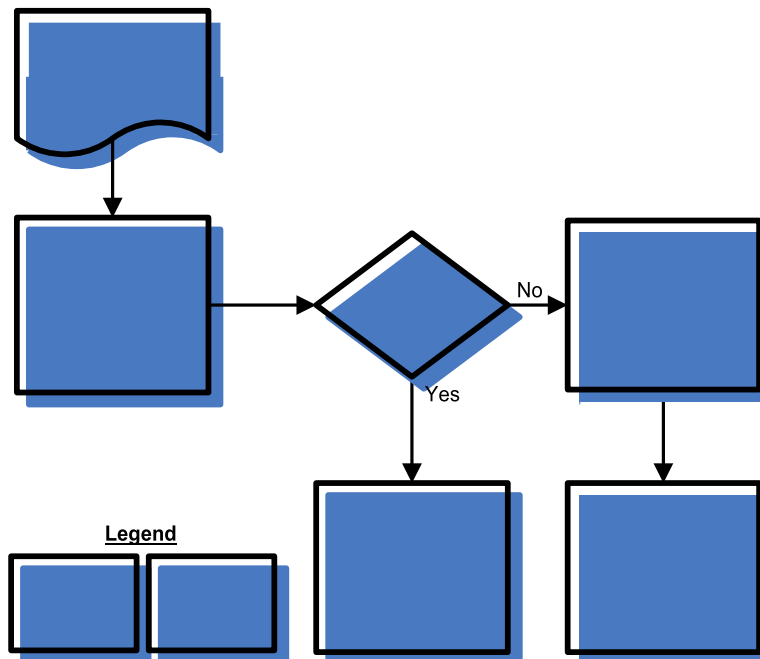
**Step 2.** The ISSO will create draft POA&Ms in CSAM for weaknesses that present unacceptable risk to the AO. POA&Ms will be developed based on the requirements outlined in section 7.7. Also see sections 7.3.3 and 7.3.4.

a. The SO in coordination with the ISSO will proceed with the POA&M Initiation process (see section 7.3).

**Step 3.** No POA&Ms will be developed for weaknesses deemed to present acceptable risk to the AO. The SO in coordination with the ISSO will proceed with Risk Acceptance process (see section 7.2).

Figure 1 depicts the POA&M Identification process.

**Figure 1 - POA&M Identification and Next Steps**



### 7.3 Risk Acceptance

The Risk Acceptance process occurs simultaneously with the POA&M Initiation process.<sup>1</sup> It should be noted that the AO(s) may choose to accept weakness risk apart from those that the SO specifically requested. Therefore, different actions in CSAM will be required depending on the POA&M process stage (Identification, Initiation or Management) in which the AO(s) decides to accept weakness risk. These processes are outlined below:

- Step 1.** The SO will request AO(s) approval for risk acceptance of weaknesses using the template “SO Risk acceptance request memo template - Draft.doc.”
  - Step 2.** The AO(s) will review risk acceptance requests.
  - Step 3.** The SO in coordination with the ISSO will respond to AO(s) requests and/or recommendations regarding risk acceptance.
  - Step 4.** The AO(s) will document risk acceptance using the template “AO Risk acceptance memo template.doc.” The AO(s) will provide the documented risk acceptance to the SO.
  - Step 5.** If a POA&M exists to address a risk that the AO(s) later accepted, the ISSO should first attempt to delete the POA&M from CSAM. If the POA&M cannot be deleted, it should be cancelled in coordination with the NESDIS CID. See section 7.3.6 for more information on POA&M removal and cancellation.
  - Step 6.** The ISSO will upload the AO-approved risk acceptance to CSAM.
    - a.** If one or more POA&Ms must remain in CSAM as described in Step 5, upload the risk acceptance document and cross-reference it according to the options and procedures described in section 7.5.5.
    - b.** If no POA&M exists for the weakness, upload the risk acceptance document as described in section 7.5.5.2.
  - Step 7.** The NESDIS CID will review CSAM weekly to identify any POA&Ms that require cancellation due to risk acceptance (see section 7.3.10). The NESDIS CID will conduct Independent Verification and Validation (IV&V) of the POA&M using section 7.7. The NESDIS CID will provide the results of the review within
-

<sup>1</sup> See NESDIS *Continuous Monitoring Planning Policy and Procedures*, NESDIS *Policy and Procedures for Conducting Security Controls Assessments* for specific requirements on obtaining AO approval of POA&Ms or accepting risk through revision of the FIPS 200.

five business days, by updating the status in CSAM. It should be noted that only the NESDIS CID may update the status of POA&Ms in CSAM to “Cancel Approved,” “Cancel Denied,” “POA&M Approved” and “Approval Denied.”

- a. If all requirements for documenting acceptable risk are met, the NESDIS CID will approve cancellation requests by changing the approval status in CSAM to “Cancel Approved.”
- b. If the POA&M does not meet requirements, the NESDIS CID will update the approval status to “Cancel Denied” with a comment explaining the reason for denied cancellation (see section 7.6). Within three business days, the ISSO will perform required modifications and reissue the cancellation request as in Step 5. The NESDIS CID will conduct a follow-up review and, if all requirements are met, approve the cancellation request as in Step 7a.

## **7.4 POA&M Initiation**

POA&Ms that address high risk undergo a different initiation process than those addressing low and moderate risk. This is because the AO(s) must approve in writing, the strategy and schedule identified in POA&Ms addressing high-risk weaknesses. The processes are outlined in the next two sections.

Please note that POA&Ms with an approval status of “Draft – Created,” “Draft – Approval Requested,” and “Approval Denied,” will be auto-approved in CSAM if required actions are not completed in a timely manner (see section 7.6). The NESDIS CID has a zero-tolerance policy in regard to POA&M auto-approvals as auto-approved POA&Ms indicate that the NESDIS CID is not taking an active role in the POA&M process. The SO or authorized delegate is responsible for monitoring progress of POA&Ms with this approval status to prevent auto-approval. The NESDIS CID will monitor progress of POA&Ms with this approval status.

### **7.3.1 Low and Moderate Risk Weaknesses**

- Step 1.** Within 10 days of POA&M creation, the ISSO will submit the POA&M for NESDIS CID IV&V by updating the status of the POA&M to “Draft – Approval Requested.” If a POA&M was created in error, the ISSO should first attempt to delete the POA&M in CSAM. If the POA&M cannot be deleted, it can be cancelled in coordination with the NESDIS CID. See section 7.3.6 for more information on deletion and cancellation.

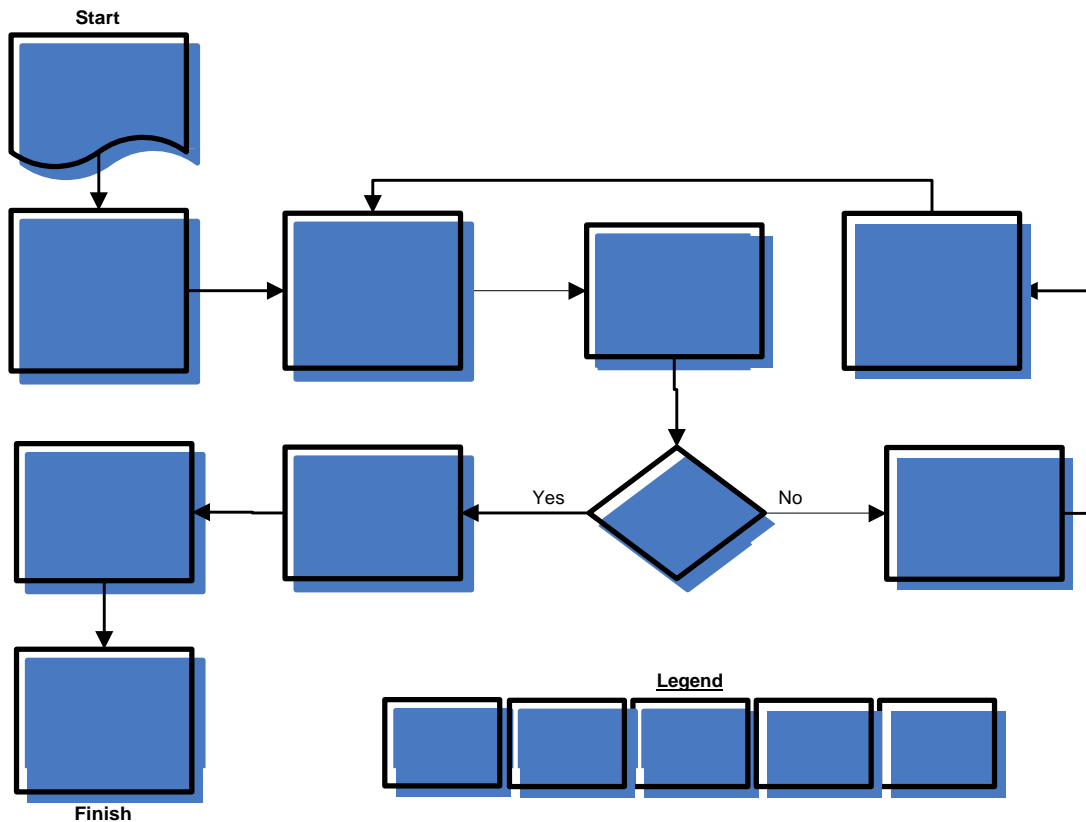


- Step 2.** The NESDIS CID will review CSAM weekly for POA&Ms that require review (see section 7.3.10). The NESDIS CID will conduct IV&V of the POA&M using section 7.7. The NESDIS CID will provide the results of the review in CSAM within five business days. It should be noted that only the NESDIS CID may update the status of POA&Ms in CSAM to “POA&M Approved” and “Approval Denied.”
- a. The NESDIS CID will update the status in CSAM to “POA&M Approved,” if the POA&Ms meet all requirements (see section 7.6).
  - b. For POA&Ms that do not meet all requirements, the NESDIS CID will update the status in CSAM to “POA&M Denied” and include a comment with the rationale (see section 7.6).
  - c. The ISSO will perform required modifications and update the POA&M status as in Step 1 within five business days. The NESDIS CID will conduct a follow-up review and update the POA&M status to “POA&M Approved” or “POA&M Denied” within three business days. The ISSO will perform required modifications and update the POA&M status as in Step 1 within three business days.

The following steps must be completed within 10 business days of POA&M identification:

- Step 3.** The SO will inform the AO(s) of all low and moderate risks in accordance with the *NESDIS Policy and Procedures for Conducting Security Controls Assessments*.
- Step 4.** The AO(s) will review and approve PO&AM completion dates for all low and moderate risks to the system.

Figure 2 - POA&M Initiation for Low to Moderate Risk Weaknesses



### 7.3.2 High Risk Weaknesses

- Step 1.** Within 10 days of POA&M creation, the ISSO will notify the NESDIS CID of POA&Ms that are ready for IV&V. The ISSO will include the CSAM IDs of POA&Ms requiring review in an email message (encrypted as required) addressed to [nesdis.it.security@noaa.gov](mailto:nesdis.it.security@noaa.gov). If a POA&M was created in error, the ISSO should first attempt to delete the POA&M in CSAM. If the POA&M cannot be deleted, it can be cancelled in coordination with the NESDIS CID. See section 7.3.6 for more information on deletion and cancellation.
- Step 2.** The NESDIS CID will conduct IV&V of the POA&M using the section 7.7. The NESDIS CID will provide the results of the review to the SO and ISSO within five business days.

- a. The NESDIS CID will advise the ISSO and SO that they should proceed with AO(s) review of POA&Ms that meet all requirements (Steps 3 and 4).
- b. The NESDIS CID will notify the ISSO and SO if POA&Ms need modification.
- c. The ISSO will perform required modifications and notify the NESDIS CID and SO within five business days. The NESDIS CID will conduct a follow-up review and provide the results of the review to the SO and ISSO, within three business days. The ISSO will perform any required modifications and notify the NESDIS CID and SO within three business days.

Steps 3 and 4 will be completed within 10 business days of POA&M identification:

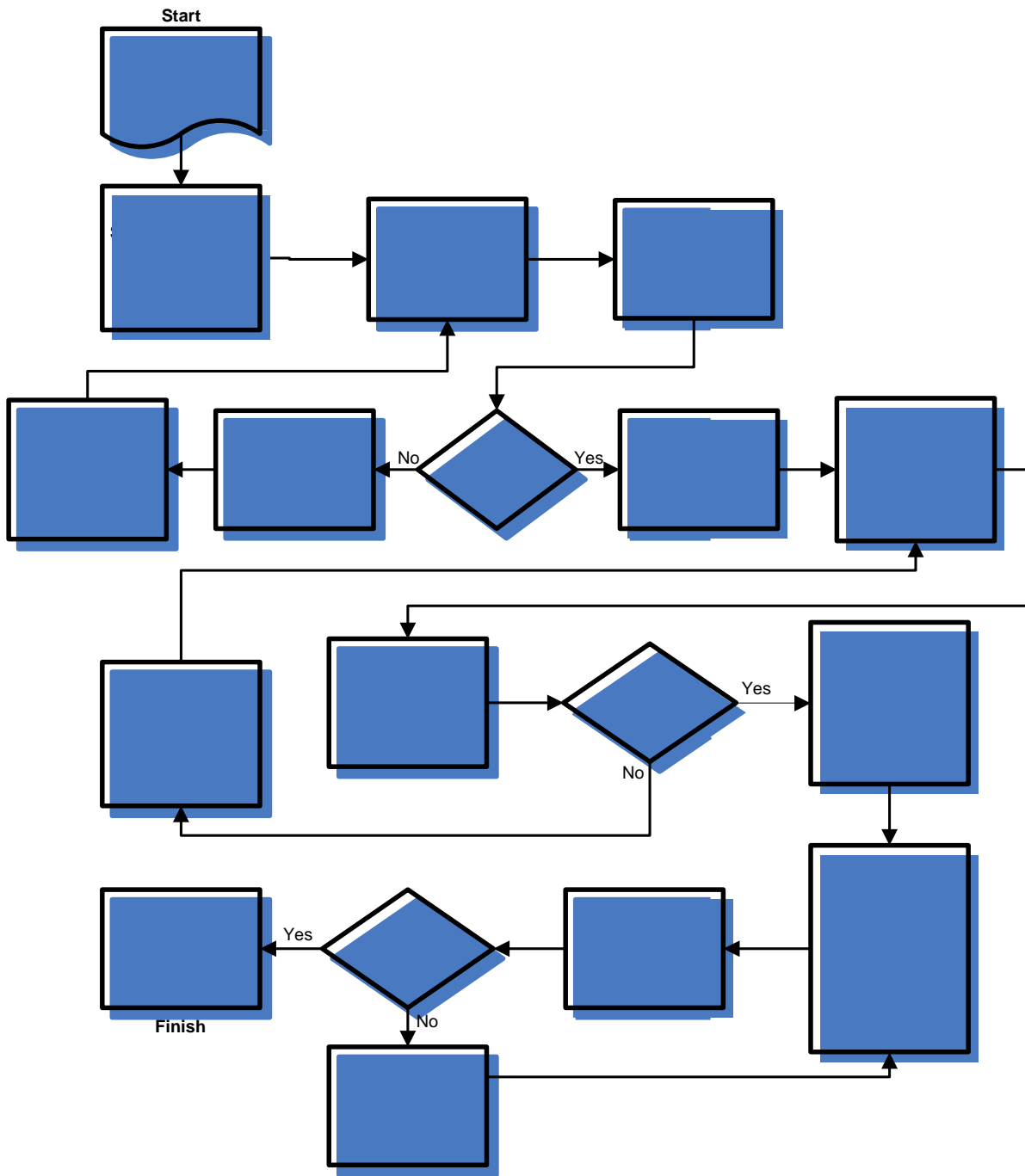
- Step 3.** The SO will inform the AO(s) of all high risks to the system in accordance with the NESDIS Policy and Procedures for Conducting Security Controls Assessments. The SO will request that the AO(s) approves POA&Ms that address high risk using the template “SO High Risk POA&M approval request memo template - Draft.doc.”
- Step 4.** The AO(s) will review all high risks to the system.
- a. The AO(s) will provide the SO written approval of POA&Ms addressing high risk using the template “AO High Risk POA&M approval memo template - Draft.doc.”
  - b. The SO in coordination with the ISSO will respond to AO(s) requests and/or recommendations regarding POA&Ms that address high risk and notify the AO(s) upon completion. The AO(s) will proceed with documenting approval of POA&Ms that address high risk as in Step 4a.
- Step 5.** Within three business days, the ISSO will upload documented AO(s) approval of POA&Ms that address high risk (see section 7.5.5 for upload options). The ISSO will submit the POA&Ms for NESDIS CID IV&V by updating the POA&M approval status to “Draft - Approval Requested” (see section 7.6).

- Step 6.** The NESDIS CID will review CSAM weekly to identify POA&Ms for review: AO-approved POA&Ms that address high risk (see section 7.3.10). The NESDIS CID will conduct IV&V of the

POA&M using section 7.7. The NESDIS CID will provide the results of the review within five business days, by updating the status in CSAM. It should be noted that only the NESDIS CID may update the status of POA&Ms in CSAM to “POA&M Approved” and “Approval Denied.”

- a.** The NESDIS CID will change the approval status in CSAM to “POA&M Approved” if the AO(s) documented approval has been provided in CSAM.
- b.** If the POA&M does not meet requirements, the NESDIS CID will update the approval status to “Approval Denied” with a comment explaining the reason for denied approval (see section 7.6). Within three business days, the ISSO will make the necessary updates and submit the POA&M for review as in Step 5. The NESDIS CID will conduct a follow-up review and, if all requirements are met, approve the POA&M in CSAM as in Step 6a.

Figure 3 - POA&M Initiation for High Risk Weaknesses



Legend



### 7.3.3 Add POA&M in CSAM

To add a new POA&M to CSAM, you must first create a blank record and then update the new record. Please note that a user must have the Primary Author or Author role to add POA&M items in CSAM. See the supplementary document *Getting Started with the Cyber Security Assessment and Management (CSAM) Tool* for a discussion of CSAM roles.

Follow the steps below to add a POA&M item in CSAM:

- Step 1.** While in CSAM, select “POA&Ms” in the top menu.
- Step 2.** In the upper right corner of the form, select the link “Add POA&M.”
- Step 3.** Select or verify the SSP desired.
- Step 4.** Leave “Program” blank.
- Step 5.** Select the “Create POA&M” button.
- Step 6.** Proceed to the next section to begin updating the new POA&M.

### 7.3.4 Update POA&M in CSAM

The steps outlined in this section are the same for updating a new POA&M (added using steps in previous section) and updating an existing POA&M. Please note that the Primary Author or Author roles in CSAM are required to update a POA&M in CSAM. See the supplementary document *Getting Started with the Cyber Security Assessment and Management (CSAM) Tool* for a discussion of CSAM roles.

#### 7.3.4.1 POA&M Search

The POA&M search form is the main access point for adding, updating, and viewing POA&Ms. It includes a form that provides many options for viewing and filtering POA&M data.

Follow the steps below to access the POA&M search form:

- Step 1.** While in CSAM, select “POA&Ms” in the top menu.
- Step 2.** You are now at the POA&M search form and can do a search on all POA&Ms or set specific parameters to filter search results.

**Step 3.** When you have selected all the parameters desired  
(maintaining the form default values will bring up all



system POA&Ms for which you have access), select “Submit” in the lower left corner of the POA&M form.

**Step 4.**

The search results will appear in a table below the form. To sort on a column, select the column heading.

**Step 5.** For viewing or updating POA&Ms, select the five-digit POA&M ID in the first column of each result row.

**Step 6.** Depending on your browser, a new tab or window will appear with the POA&M General tab as the default view.

### 7.3.4.2 POA&M General Tab

Follow the steps below to update the POA&M General tab:

**Step 1.** Select “Edit” in the lower left corner of the POA&M General tab.

**POA&M GENERAL** Associations Milestones

NOAA5003 - Geostationary Operational Environmental Satellite (GOES) Ground System

POAM ID: 32131 POAM Title:

POAM Seq: 116

Detailed Weakness Description

Status	Not Started
Severity	no entry
CSAM Derived Criticality	
User Identified Criticality	no entry
Cost	
Assigned	
Assigned Date	
Artifacts	Total: 0

Date	By
Draft - Created	2/21/2009   Nadine Haddad

Due Date	Start	Finish
Planned		
Actual		

Delay Reason: no entry

Weakness

Exclude from OMB Reporting

Accepted Risk

**1**

Edit

**Step 2.** Update the following fields. Requirements for each field are outlined in section 7.7.

- a.** POA&M Title (The POA&M Title must include the control association, such as (MA-4).)


- b. Weakness Description
- c. Risk Level is specified in the User Identified Criticality field
- d. Cost (If no cost is specified, an explanation of cost should be included in the weakness comments. See section 7.3.4.4 for guidance.)
- e. Due Date
- f. Assigned (Select individuals name, usually the SO. If the individual is not in the list you can add a new point of contact using steps in section 7.3.4.5.)

**Step 3.** Select “Save” in the lower left corner of the POA&M General tab to save all changes.

The screenshot shows the 'POA&M GENERAL' tab of a software interface. At the top, there are tabs for 'Associations' and 'Milestones'. Below the tabs, the form displays 'NOAA5000 -' and fields for 'POAM ID: 32131', 'POAM Seq: 116', and 'POAM Title:'. A large text area for the 'Detailed Weakness Description' is present, with a 'Full Screen Edit' link. Below this, there are several sections: 'Status' (Not Started), 'Severity' (no entry), 'CSAM Derived Criticality', 'User Identified Criticality' (Very Low), 'Cost' (empty), 'Assigned' (-Select POC-), 'Assigned Date', and 'Artifacts' (Total: 0). A 'Weakness' checkbox is checked, and there are options to 'Include from OMB Reporting' and 'Accepted Risk'. On the right side, there are fields for 'Date' (Draft - Created 2/21/2009), 'By', and a 'Submit' button. Below that, there are 'Due Date' (TBD), 'Start' (TBD), 'Finish' (TBD), 'Planned' (TBD), 'Actual' (TBD), and 'Delay Reason' (-No Selection-) fields. At the bottom left, there are 'Save', 'Delete', and 'Cancel' buttons. Annotations 'a' through 'f' and '3' are placed on the form to highlight specific elements.

### 7.3.4.3 Source

Follow the steps below to record the source of the weakness:

**Step 1.** In the **POA&M General** tab and next to the Weakness checkbox, select the notepad icon (  ). A new window will open.

**Step 2.**

In the new window, select the “Add Comment” link.

**Step 3.** In the text box, enter the source and include the name/type and a specific date (e.g., Source: C&A 1/1/2009; OIG Report 12345, 12/1/2009)


**Step 4.** Select “Update.”

**Step 5.** The text that was just added will appear in the “Weakness Comments” table.

**Step 6.** Close the window when complete.

#### 7.3.4.4 Cost Comments

Follow the steps below to include an explanation of cost:

**Step 1.** In the **POA&M General** tab and next to the Weakness checkbox, select the notepad icon (  ). A new window will open.

**Step 2.** In the new window, select the “Add Comment” link.

**Step 3.** In the text box, enter an explanation of cost including the anticipated source of funding (e.g., “Resource Estimate: Existing staff level of effort”).

**Step 4.** Select “Update.”

**Step 5.** The text that was just added will appear in the “Weakness Comments” table.

**Step 6.** Close the window when complete.

#### 7.3.4.5 Adding a Point of Contact in CSAM

If you have the Primary Author role, you can add a point of contact to CSAM by following the steps below:

**Step 1.** While in CSAM, select “Assessments” in the top menu.

**Step 2.** Select “Add POC to Picklist.”

**Step 3.** Populate, at minimum, the Name, Phone, and Email fields.

**Step 4.** Select “Insert”. Please note that the newly added name may not show in the pick list unless you close and then reenter the screen you are selecting from.

### 7.3.4.6 Security Control Mapping

Follow the steps below to associate a security control to a POA&M:

- Step 1.** Select the **Associations** tab.
- Step 2.** Select the Edit button in the lower left corner of the **Associations** tab.
- Step 3.** A scroll box will appear with NIST 800-53 controls listed. Scroll through the list and select the checkbox next to each control that applies (for more information on security controls, please consult NIST SP 800-53 Rev. 2 Recommended Security Controls for Federal Information Systems at the NIST website: <http://csrc.nist.gov/publications/PubsSPs.html>).
- Step 4.** Select “Save.”

### 7.3.4.7 POA&M Milestones Tab

Follow the steps below to add a milestone:

- Step 1.** Select the **Milestones** tab.
- Step 2.** Select the “Add” link.
- Step 3.** Update milestones description (Note: CSAM will add a number to each milestone in the order it is added. Also, if a milestone is removed, the milestone numbers assigned will not be reordered. For example, if one removes milestone 3 out of 5, the remaining milestones will be numbered 1, 2, 4 and 5). Each POA&M must have at least two milestones.
- Step 4.** Update “Assigned To”. Select from the drop-down menu the first and last name of the individual responsible for completion (usually the ISSO).
- Step 5.** Update “Due Date” with the planned completion date for the milestone (Note: Due Date defaults to the current date).

**Step 6.** Update Planned Start and Planned Finish with the appropriate date as approved by the AO.

**Step 7.** Select the “Update” link.

**Step 8.** For all high-risk POA&Ms resulting from certification and accreditation of a high-impact NESDIS system, an additional milestone is added for “AO review and concurrence.” Due to the impact on the agency-wide risk posture, validation of POA&M closure is performed on a 100% basis by NESDIS CID, and NESDIS CID tracks milestone progress for these POA&Ms and reports status to the AO monthly. The Description for the milestone is “AO review and concurrence.” The SO must notify the NESDIS CID via e-mail at [nesdis.it.security@noaa.gov](mailto:nesdis.it.security@noaa.gov) that the POA&M is ready for AO review. The Planned Start date is the day after the Planned Finish of the last SO milestone. The Planned Finish is 30 days after the Planned Start date if the POA&M pertains to anything other than development of a new system module/subsystem that will replace an existing component that does not provide adequate security. If the POA&M pertains to development/redesign of a major component of a system, then the AO review milestone is 90 days. Usually the POA&Ms requiring new system development involve the Office of Systems Development (OSD).

### **7.3.5 Update Status**

Please see section 7.6.

### **7.3.6 Remove or Cancel a POA&M**

A POA&M can be deleted from CSAM if the approval status is “Draft – Created.” If the POA&M has an approval status of “POA&M Approved” or “Auto Approved” it cannot be deleted. However, it can be removed through cancellation. This must occur in coordination with the NESDIS CID.

#### **7.3.6.1 Remove a POA&M**

Follow the steps below to remove a POA&M:

**Step 1.** Search for the POA&M you want to remove by following the steps outlined in section 7.3.4.1.

**Step 2.** Select the Edit button in the lower left corner of the



NESDIS Quality Procedure [NQP] – 3409  
Revision 2.1

Effective Date: September 28, 2012  
Expiration Date: Until Superseded

**POA&M General tab.**

- Step 3.** Select the Delete button in the lower left corner of the **POA&M General** tab.
- Step 4.** A confirmation dialogue box will appear. Select “OK.”
- Step 5.** A message will appear confirming that the POA&M has been deleted and that you may close the window

### 7.3.6.2 Cancel a POA&M

Follow the steps below to cancel a POA&M:

- Step 1.** Search for the POA&M you want to cancel by following the steps outlined in section 7.3.4.1.
- Step 2.** Select the Edit button in the lower left corner of the **POA&M General** tab.
- Step 3.** Update the approval status to “Draft – Approval Requested.” Inform the NESDIS CID about the reason for the approval request.
- Step 4.** The NESDIS CID will change the approval status to “POA&M Approved” and include a comment explaining the reason for the approval (e.g., “POA&M created in error. Approving for subsequent cancellation.”).
- Step 5.** Update the approval status to “POA&M Cancellation Requested” and include a comment explaining the reason for cancellation (e.g., “POA&M created in error.”)
- Step 6.** The NESDIS CID will change the approval status to “Cancel Approved” and include a comment explaining the reason for cancellation (e.g., “POA&M created in error.”)

### 7.3.7 Sensitive Information

The POA&M is a high-level management tool. Sensitive data should be excluded from POA&M descriptions and instead be restricted to artifacts uploaded to support the POA&M identification or closure. If sensitive data is included in the weakness narratives, the POA&M should note the fact of its special sensitivity. Sensitive data includes:

- Passwords
- IP Addresses

- Open ports
- Specific information about intrusion detection systems
- Specifics regarding firewall rules
- Any details that could directly jeopardize the security of the system

### 7.3.8 Scheduled Completion

When developing POA&M mitigation schedules, the AO, SO, and ISSO should consider the following timeframes, unless otherwise specified by the NESDIS CID or the National Oceanic and Atmospheric Administration (NOAA). See the NOAA *IT Security Manual*, 212-1302, Appendix E for more information on the NOAA Vulnerability Notification and Priority levels. Critical vulnerabilities are normally communicated via US-CERT/DOC/NOAA data calls and are expected to be mitigated within three days. High risk scan vulnerabilities must be mitigated within 30 days.

Medium risk scan vulnerabilities must be mitigated within 90 days (before the next quarterly scan). Low risk scan vulnerabilities must be mitigated within 120 days or may be candidates for risk acceptance along with “warning” level vulnerabilities. It is recommended that other High-risk vulnerabilities be mitigated within one year.

**Table 1 – Mitigation of Scan Vulnerabilities**

Risk Level	Mitigated within
Critical (NOAA Priority 1)	3 days
High (NOAA Priority 2)	30 days
Medium (NOAA Priority 3)	90 days
Low	120 days

If a mitigation of a weakness cannot occur within the specified timeframes, this may indicate the existence of an underlying issue. In turn, the underlying issue should be included in a POA&M for mitigation.

Mitigation schedules that exceed required timeframes above must have a documented rationale. AO risk acceptance may also be a considered for weaknesses that cannot be mitigated within one year.

### 7.3.9 Consolidated Reporting

The POA&M is a process for identifying and correcting weaknesses in the IT environment. The focus on weakness correction means that a careful

assessment of both the individual weakness and the correction of that weakness are essential for cost effective management. Since multiple weaknesses may have a single correction, the following rules apply.

Weaknesses with a common corrective action will be consolidated into a single POA&M. Also, if the mitigation of one weakness (Weakness A) is dependent on the corrective action of another (Weakness B), the dependent weakness (Weakness A) can be included in the POA&M of the other (Weakness B).

In order to accomplish consolidation:

**Step 1.** Logically group the candidate weaknesses based on common corrective action(s).

**Step 2.** Further subdivide these groups according to risk level.

**Step 3.** Add a new POA&M to CSAM for each group identified in step 2 using the following guidelines (see section 7.3.3). See section

7.7 for additional field format and content requirements.

- a. Combine and summarize unique weakness descriptions in the consolidated POA&M.
- b. Combine and summarize unique weakness sources.
- c. Update the Cost field to reflect combined cost for mitigation of multiple weaknesses.

If existing POA&Ms will be consolidated, use Steps 1-3 above and follow these additional steps:

**Step 4.** Cancel the POA&Ms to be consolidated. Include a comment with the cancellation request that provides the reason/justification for cancellation and a cross-reference to the new consolidated POA&M. (e.g., Based on NESDIS CID guidance, weaknesses with common corrective actions may be consolidated into one POA&M. The action in POA&M ID #44444 to implement XYZ software, will also mitigate the weakness described in this POA&M. Therefore this weakness has been consolidated into POA&M ID #44444.)

**Step 5.** Create a file that cross references the IDs of all the POA&Ms that are being canceled. Include the label “XRefP” in the file name to indicate that the file contains cross references to other POA&Ms. For example, The file “XRefP-LinuxAdobe.txt”

contains the text “This POA&M rolls-up canceled POA&Ms 12345, 67890, 54321, and 09876.” Upload the text file to the new consolidated POA&M using Steps 6-10.

- Step 6.** In the **POA&M General** tab and next to the “Artifacts” label, select the link “Total:”
- Step 7.** A new window will open. In the new window, select the “Add Artifact” link.
- Step 8.** In the file field that appears, select “Browse” and locate the file to upload.
- Step 9.** Double click the file or select “Open.”
- Step 10.** Select the “Upload” link. The file will now be listed on this page.

### 7.3.10 Identify POA&Ms for Review

Use the POA&M search form to identify new POA&Ms for review that are in a “Draft – Approval Requested” or “POA&M Cancellation Requested” approval state.

- Step 1.** While in CSAM, select “POA&Ms” in the top menu.
- Step 2.** You are now at the POA&M search form.
- Step 3.** For Approval Status field, select “Draft – Approval Requested” or “POA&M Cancellation Requested.”
- Step 4.** Select “Submit.”
- Step 5.** The search results will appear in a table below the form.
- Step 6.** Select the five-digit POA&M ID in the first column of each result row to begin reviewing the POA&M. Depending on the type of browser, a new browser tab or window will appear with the **POA&M General** tab as the default view.

## 7.4 POA&M Management

The SO and ISSO are responsible for monitoring progress of corrective actions in CSAM. The ISSO and those assigned will update milestone due dates and POA&M due dates in CSAM on or before dates occur (see section 7.3.4).

At the end of each month the NESDIS CID will download data from CSAM to assess POA&M performance of the previous month. The NESDIS CID will evaluate completion, for each system, based on the POA&M due date. The total number of POA&Ms over 120 days delayed will be identified for each system. Also, only those POA&Ms in a “Close Approved” state will be considered closed. POA&Ms in a “Close Requested” state will be considered open (see section 7.6).

### **7.4.1. Tracking Tools**

Those involved in the POA&M process have several tools at their disposal for tracking POA&Ms in CSAM. These include the CSAM Start Page, the POA&M Search Form, and POA&M reports.

#### **7.4.1.1 CSAM Start Page**

The CSAM start page is the first page a user sees after logging into CSAM. In the bottom half of the page, late POA&Ms are identified along with filtering options. Please note that POA&Ms with an approval status of “Cancel Approved”, “Approval Denied”, and “Draft – Created”, including those that are past due, will not be included in this list. Because of this, the start page may not be an accurate indicator of corrective action status.

#### **7.4.1.2 POA&M Search Form**

The POA&M search form is the main access point for adding, updating, and viewing POA&Ms. It includes a form that provides many options for viewing and filtering POA&M data. To access the POA&M search form please see section 7.3.4.1.

#### **7.4.1.3 POA&M Reports**

The POA&M reports feature in CSAM provides the option to download POA&M data (POA&M descriptions, milestone descriptions, and scheduling information) in various file formats.

Follow the steps below to download a POA&M report:

- Step 1.** While in CSAM, Select “SSP Contents” in the top menu.



- Step 2.** Select the SSP in the SSP List for which you would like to download a report.
- Step 3.** Select reports in the top menu.
- Step 4.** Select POA&M.
- Step 5.** Select the field options you prefer.
- Step 6.** Download, save, and open the report.

#### 7.4.1.4 Tasks

The tasks report is useful for tracking POA&M and milestone completion. To view the report, select the “Task” link above the top menu. The tasks report lists the total number of POA&Ms and milestones that are due for completion at various intervals. The report also contains a drill-down feature to identify specific POA&Ms and milestones that contribute to the values specified in the report.

### 7.5 POA&M Completion

POA&Ms that address high risk undergo a different process than those addressing low and moderate risk. This is because the AO(s) must concur with closure actions for POA&Ms addressing high-risk weaknesses. These processes are described in the next two sections.

#### 7.5.1 Low to Moderate Risk Weaknesses

- Step 1.** On behalf of the SO, the ISSOs implement and assess closure of the corrective actions for their system-level POA&Ms and upload documented evidence of POA&M closure testing in CSAM. The methodology followed must comply with assessment procedures in NIST SP 800-53A for the control associated with the POA&M.
- Step 2.** The ISSO will update the POA&M to report closure (see section 7.5.4) and update the status in CSAM to “Close Requested” (see section 7.6) 15 days prior to the POA&M scheduled completion date. This is to allow time for the SO to assess closure.
- Step 3.** The ISSO will upload complete evidence (see NIST SP 800-53A for the associated control to determine sufficient and relevant evidence of Interviews, Examinations, and/or Tests required) supporting closure to CSAM within five business days that the

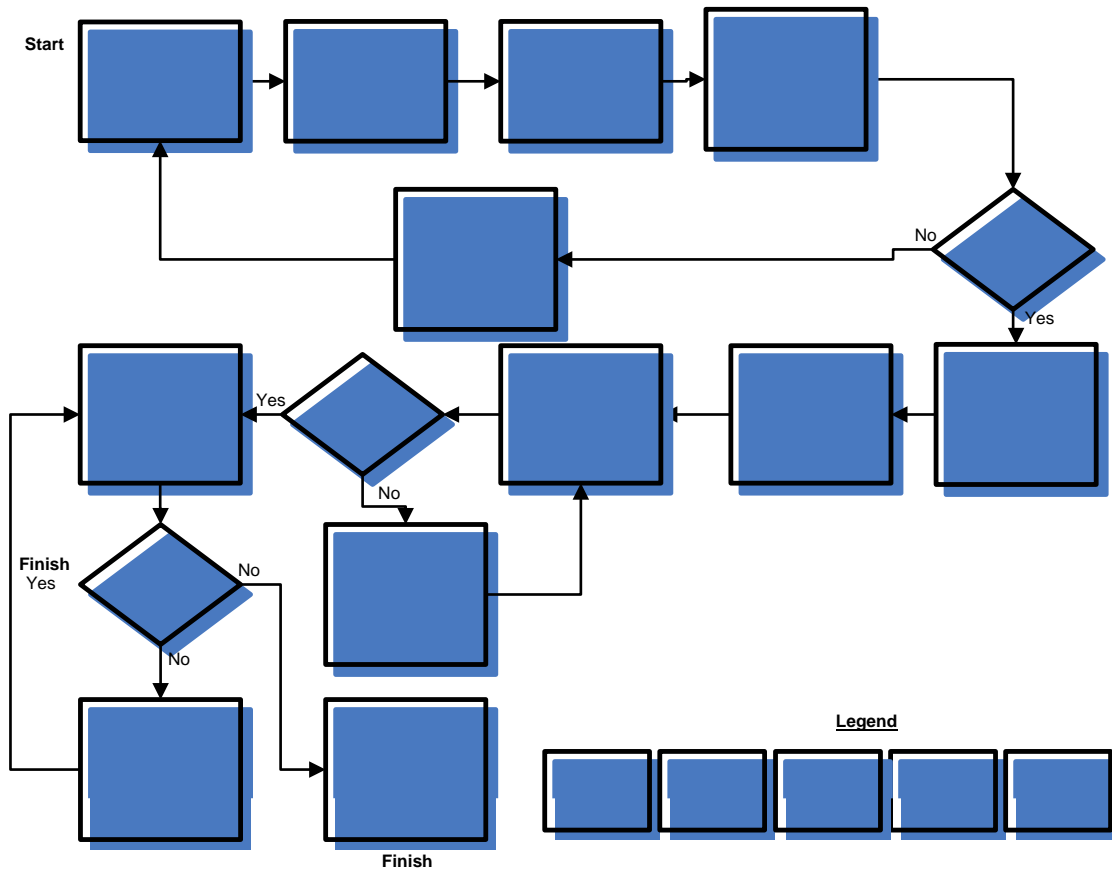
POA&M approval status was changed to “Close Requested” (see section 7.5.5). This way, NESDIS CID validators will have ready access to the evidence to evaluate its adequacy without interrupting personnel or system-level operations.

- Step 4.** At least monthly, SOs (or their authorized delegate) identify in CSAM all POA&Ms in the following categories: POA&Ms that address low risk with a status of "Close Requested;" and POA&Ms that address moderate risk with a status of “Close Requested.” CSAM can produce a report of the POA&Ms with this status (see section 7.3.4.1). The SO (or their authorized delegate – Note: the authorized delegate for POA&M closure cannot be the same as the person who requested POA&M closure on behalf of the SO) must review evidence of POA&M closure (see section 7.5.3) to ensure adequate testing has been performed and documented to support POA&M closure, and if adequate, update the POA&M status to “Close Approved” (see section 7.6). SOs should develop their own internal procedure to allow this review to take place and should be prepared to share this procedure in the event of an audit.
- Step 5.** NESDIS CID will verify and validate monthly, on a sampling basis, the adequacy of evidence supporting POA&Ms closed in the prior month (i.e., in April a sample of POA&Ms closed in March will be evaluated). The following process will evolve over the duration of a month, and will recur monthly:
- a. The NESDIS CID will provide the SO with notification of POA&Ms selected for the monthly IV&V at the start of their review, by the fifth business day of the month (i.e., early start is the first of the month, late start is the fifth business day of the month).
  - b. The NESDIS CID will check POA&Ms selected for IV&V for availability of evidence.
  - c. If the evidence of closure is not available to the validators in CSAM, the SO will have three business days from selection notification (see Step 5a) to provide the reviewer access to the evidence in either hard or soft copy format.
  - d. The NESDIS CID will complete their review (see section 7.5.3) within 10 business days of SO notification and will provide the SO with written feedback of the results of their review within five business days of review completion.
  - e. If the written feedback reflects that CID does not concur with the POA&M closure, then SOs will be permitted five business days to respond and provide additional evidence

(about the end of the third week of the month).

- f. If closure is not resolved after reviewing additional evidence, CID will discuss the vulnerability with the SO and AO and new POA&M may need to be created to address unmitigated vulnerabilities depending on the AO's determination.

**Figure 4 - POA&M Completion for Low to Moderate Risk Weaknesses**



### 7.5.2 High Risk Weaknesses

For all high-risk POA&Ms resulting from certification and accreditation of a high-impact NESDIS system, an additional milestone is added for “AO review and concurrence.” Due to the impact on the agency-wide risk posture, validation of POA&M closure is performed on a 100% basis by NESDIS CID, and NESDIS CID tracks milestone progress for these POA&Ms and reports status to the AO monthly. The Description for the milestone is “AO review and concurrence.” The “Assigned To” is NESDIS CID. The Planned Start date is the day after the Planned Finish of the last SO milestone. The Planned Finish is 30 days after the Planned Start date if the POA&M pertains to anything other than development of

a new system module/subsystem that will replace an existing component that does not provide adequate security. If the POA&M pertains to development/redesign of a major component of a system, then the AO review milestone is 90 days. Usually the POA&Ms requiring new system development involve the Office of Satellite and Product Operations (OSPO).

**Step 1.** On behalf of the SO, the ISSOs implement and assess closure of the corrective actions for their system-level POA&Ms and upload documented evidence of POA&M closure testing in CSAM. The methodology followed must comply with assessment procedures in NIST SP 800-53A for the control associated with the POA&M.

**Step 2.** The ISSO will upload complete evidence supporting closure to CSAM prior to the due date of the last milestone. The last milestone for POA&Ms that address high risk is for “AO review and concurrence.” Completion of this milestone is the responsibility of the NESDIS CID. ISSOs will notify the NESDIS CID when they have completed milestones up to the “AO review and concurrence” milestone.

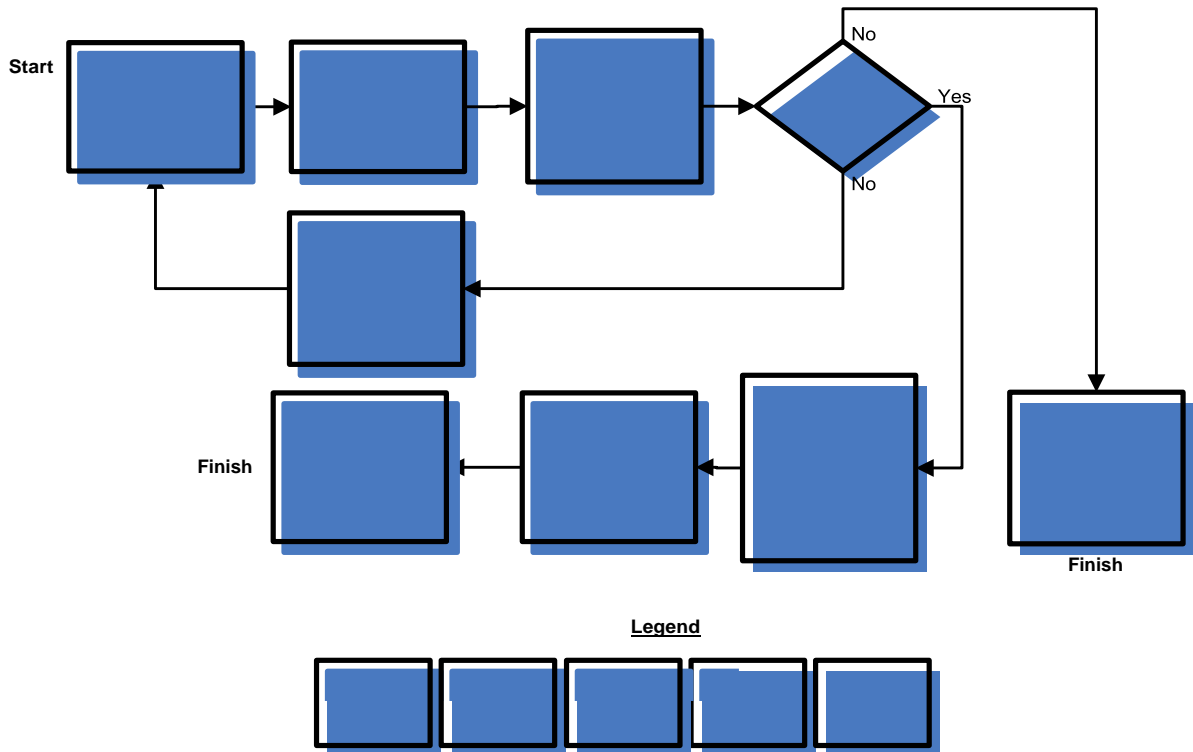
**Step 3.** As part of “AO review and concurrence,” the NESDIS CID will verify and validate the adequacy of evidence supporting closure (see section 7.5.3).

- a. If the NESDIS CID concurs with the POA&M closure, it will update the status of the “AO review and concurrence” milestone with the actual finish date within five business days (milestone updates are covered in section 7.5.4).
- b. If the NESDIS CID does not concur with the POA&M closure, it will notify the ISSO and SO within five business days. The ISSO and SO will be permitted five business days to respond and provide additional evidence.
- c. If closure is not resolved after reviewing additional evidence, the NESDIS CID will discuss the vulnerability with the SO and AO(s) and a new POA&M may need to be created to address unmitigated vulnerabilities, depending on the AO’s determination.

**Step 4.** After the “AO review and concurrence” milestone has been completed, the ISSO will update the status of the POA&M to “Close Requested” in CSAM within three business days (see section 7.6).

**Step 5.** The NESDIS CID will review CSAM for POA&M closure requests on a weekly basis. If the NESDIS CID previously concurred with the POA&M closure in Step 3, it will update the status of the POA&M to "Close Approved" in CSAM (see section 7.6).

**Figure 5 - POA&M Completion for High Risk Weaknesses**



### 7.5.3 Closure Request Review

The NESDIS CID and SO or authorized delegate will use the following method when reviewing POA&M closures. SOs will use the POA&M search to identify low and moderate risk POA&Ms for review. Follow the steps outlined in section 7.3.4.1 along with these additional guidelines:

**Step 1.** In Step 2, for the "Approval Status" dropdown menu, select the option "POA&M Close Requested."

**Step 2.** Risk level is defined in "Organizational Priority." In Step 4, click on the header "Organizational Priority" in the results table to sort this column and identify groups of low and moderate risk POA&Ms for review.

- Step 3.** The NESDIS CID will identify high-risk POA&Ms for review based on the “AO Review and concurrence” milestone. The NESDIS CID will use the “Tasks” menu to search for the “AO review and concurrence” milestones (see section 7.4.1.4) that are coming due and perform the closure review.
- Step 4.** After identifying POA&Ms for closure review, review the POA&M, including milestones and source. POA&Ms developed prior to this policy may have not had a quality review.
- Therefore, it may be necessary to review the source report to ensure that the POA&M will address the finding.
- Step 5.** Review the closure request comments.
- Step 6.** Evaluate the evidence to see if it provides validation of closure.
- In general, the same evaluation method that uncovered the weakness should be used to ensure it was mitigated. The type of evidence required will depend on how the weakness was identified:
- a.** If the source indicates that the weakness was identified through developer Security Test and Evaluation (ST&E), annual independent Security Controls Assessment (SCA), or the Security Assessment Report (SAR), NIST 800-53A testing is required and the evidence should substantiate that this testing has occurred. Artifacts of ST&E and SCA testing would include one or more of the following:
    - i.** Screen shots of testing
    - ii.** Detailed testing notes
    - iii.** Written policy and/or procedures with applicable approval signatures, where a previous policy and/or procedure did not meet requirements or did not exist
    - iv.** Vulnerability scan results showing that a vulnerability no longer exists where it did previously. If the source is from vulnerability scanning, an appropriate artifact would be vulnerability scan results showing that a vulnerability no longer exists where it did previously.
- Step 7.** Determine if the closure request should be:
- a.** Approved (Change the approval status to “Close Approved”)

- b. Denied (needs more information – Change the approval status to “Close Denied”).
- c. Denied (Change the approval status to “Close Denied”), because the POA&M does not address the deficiency properly. In this case the POA&M may need to be Cancelled and replaced with a new POA&M (see sections 7.6 and 7.3.6).

#### **7.5.4 Report Closure**

- Step 1.** Search for the POA&M you want to close by following the steps outlined in section 7.3.4.1.
- Step 2.** Identify Actual Finish date for all milestones listed in the Milestones tab.
- Step 3.** Identify Actual Start date in the POA&M General tab
- Step 4.** Identify Actual Finish date in the POA&M General tab
- Step 5.** Update the approval status in the POA&M General tab to “POA&M Close Requested”.
- Step 6.** Include comments associated with that status in the field directly beneath where the status was selected.
- Step 7.** See the section 7.5.5 for a discussion of POA&M Artifacts and the options to upload them.
- Step 8.** Select “Save” when updates are complete.

#### **7.5.5 Artifacts and Supporting Files**

Artifacts can be uploaded directly to a single POA&M item or, if the artifact is shared, to another area of CSAM and cross referenced by all POA&Ms sharing it (see sections 7.5.5.2 and 7.5.5.3). CSAM only accepts specific file types. Please see the next section for more information on accepted file types and what to do for files of un-accepted types.

##### **7.5.5.1 File Types**

CSAM only accepts files with the following extensions: pdf, doc, xls, rtf, and txt. Any other files or artifacts must be maintained locally by the SO or authorized delegate and cited in CSAM using the following steps:

**Step 1.** Create a file with “ArtLoc” (short for “Artifact(s) Location”) in the file name. The contents of the file should identify where and/or who to contact to obtain the artifact(s) (e.g., “Documentation can be obtained by contacting John Doe, NOAA5007 System Owner, at johndoe@thisgov.gov.”).

**Step 2.** Upload the “ArtLoc” file using the steps in section 7.5.5.3.

### 7.5.5.2 Shared Artifacts or Files

If one artifact or file is shared by multiple POA&Ms, it can be uploaded to another area of CSAM and cross referenced using the following steps:

**Step 1.** Login to CSAM.

**Step 2.** Select SSP Contents in the top menu.

Org	SSP	POAM Title	POAM ID	Status	SCD	Days Assigned To:	Exclude from OMB
NOAA	NOAA5006 - Headquarters Information Technology Support Local Area Network	NOAA5006; AC-4, CA-3 and	32658	Delayed	12/1/2007	-506 Charles MacFarland	No
NOAA	NOAA5023 - Search and Rescue Satellite Aided Tracking	NOAA5023-2008-49; Not Ful	27303	Delayed	7/31/2008	-263 Ajay Mehta	No
NOAA	NOAA5045 - NOAA Environmental Satellite Processing Center	NOAA5045-2007-51; 800-53:	28168	Delayed	1/30/2009	-80 Kathy Kelly	No
NOAA	NOAA5045 - NOAA Environmental Satellite Processing Center	NOAA5045-2007-14; 800-53:	28179	Delayed	1/30/2009	-80 Kathy Kelly	No
NOAA	NOAA5004 - Wallops Command and Data Acquisition - Data Collection System	NOAA5004A - Data General	32696	Delayed	3/31/2009	-20 Gary Davis	No
NOAA	NOAA5026 - Polar Operational Environmental Satellite Ground System	C&A TTS:The Test and Trai	32292	Delayed	3/31/2009	-20 Kathy Kelly	No
NOAA	NOAA5040 - Comprehensive Large Array-data Stewardship System	NOAA5040-2008-212 Linux p	33711	Planned/Pending	4/10/2009	-10 Rick Vizbulis	No
NOAA	NOAA5040 - Comprehensive Large Array-data Stewardship System	Sun hosts at NCDC show mu	33712	Planned/Pending	4/10/2009	-10 Rick Vizbulis	No
NOAA	NOAA5040 - Comprehensive Large Array-data Stewardship System	NOAA5040-2008-166; RA-5.3	27521	In Progress	4/17/2009	-3 Rick Vizbulis	No

**Step 3.** From the SSP List, select the SSP for which you would like to upload a shared artifact or file.



!!!TEST SERVER!!!

CSAMC&A Web User: Nadine Haddad [Log Out](#) [Tasks Custom Queries](#) [Help](#)

Home [SSP](#) [Contents](#) [Assessments](#) [POAMs](#) [Reports](#) [Component](#) [Department](#) [Maintenance](#)

**SSP: NOAA5003 - Geostationary Operational Environmental Satellite Ground System** [Comments](#)

[SSP List](#) [General](#) [Info](#) [Types](#) [Locations](#) [Interfaces](#) [Narratives](#) [Appendices](#) [POCs](#) [Artifacts](#) [RTM](#) [Status](#) [Tools](#)

Select an Org: All Operational Status: All ATO Status: All SSP Name wildcard:  [Add SSP](#)

SSP Name	Org	SubOrg	CI/Key	Agency Critical	PII	Financial	Type	Category	Status	ATO Status	ATO Expires	Contractor System	FISMA Reportable	Dashboard
<a href="#">NOAA5001 - Central Environmental Satellite Computer System / Satellite Active Archive - Suitland, MD</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Major App	High	Retired	Not Started	8/17/2009	<input type="checkbox"/>	<input type="checkbox"/>	
<a href="#">NOAA5003 - Geostationary Operational Environmental Satellite Ground System</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Major App	High	Operational	ATO	5/30/2011	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5004 - Wallops Command and Data Acquisition - Data Collection System</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Major App	High	Operational	ATO	3/30/2010	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5006 - Headquarters Information Technology Support Local Area Network</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	GSS	Moderate	Operational	ATO	6/27/2009	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5008 - Fairbanks Command and Data Acquisition Station Administrative Local Area Network</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	GSS	Moderate	Operational	ATO	9/29/2011	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5009 - National Climatic Data Center Local Area Network</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Major App	Moderate	Operational	ATO	6/8/2009	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5010 - National Oceanographic Data Center Ocean Data Archive and Management System and Network</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	GSS	Moderate	Operational	ATO	9/7/2010	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5011 - National Geophysical Data Center Data Archive Management and User System</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	GSS	Moderate	Operational	ATO	1/23/2010	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5016 - Integrated Program Office</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Major App	High	Operational	ATO	11/1/2010	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

**Step 4.** Select the Status menu above the SSP list.

!!!TEST SERVER!!!

CSAMC&A Web User: Nadine Haddad [Log Out](#) [Tasks Custom Queries](#) [Help](#)

Home [SSP](#) [Contents](#) [Assessments](#) [POAMs](#) [Reports](#) [Component](#) [Department](#) [Maintenance](#)

**SSP: NOAA5003 - Geostationary Operational Environmental Satellite Ground System** [Comments](#)

[SSP List](#) [General](#) [Info](#) [Types](#) [Locations](#) [Interfaces](#) [Narratives](#) [Appendices](#) [POCs](#) [Artifacts](#) [RTM](#) [Status](#) [Tools](#)

Select an Org: All Operational Status: All ATO Status: All SSP Name wildcard:  [Add SSP](#)

SSP Name	Org	SubOrg	CI/Key	Agency Critical	PII	Financial	Type	Category	Status	ATO Status	ATO Expires	Contractor System	FISMA Reportable	Dashboard
<a href="#">NOAA5001 - Central Environmental Satellite Computer System / Satellite Active Archive - Suitland, MD</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Major App	High	Retired	Not Started	8/17/2009	<input type="checkbox"/>	<input type="checkbox"/>	
<a href="#">NOAA5003 - Geostationary Operational Environmental Satellite Ground System</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Major App	High	Operational	ATO	5/30/2011	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5004 - Wallops Command and Data Acquisition - Data Collection System</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Major App	High	Operational	ATO	3/30/2010	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5006 - Headquarters Information Technology Support Local Area Network</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	GSS	Moderate	Operational	ATO	6/27/2009	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5008 - Fairbanks Command and Data Acquisition Station Administrative Local Area Network</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	GSS	Moderate	Operational	ATO	9/29/2011	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5009 - National Climatic Data Center Local Area Network</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Major App	Moderate	Operational	ATO	6/8/2009	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5010 - National Oceanographic Data Center Ocean Data Archive and Management System and Network</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	GSS	Moderate	Operational	ATO	9/7/2010	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5011 - National Geophysical Data Center Data Archive Management and User System</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	GSS	Moderate	Operational	ATO	1/23/2010	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<a href="#">NOAA5016 - Integrated Program Office</a>	NOAA	NOAA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Major App	High	Operational	ATO	11/1/2010	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

**Step 5.** Select the “Artifacts” link associated with “Miscellaneous Artifacts.” Depending on your browser, a new tab or window will appear. Please note that you must have the Primary Author role to upload artifacts to this area.

**Note:** Most artifacts will likely be included in "Miscellaneous Artifacts" however, if another status field applies, that can be used and referenced instead. For example, if the updated Contingency Plan (CP) is an artifact, then upload the latest version of the CP to this area by first selecting the "Artifacts" link associated with the CP (see "a" in the figure below). Then continue with Steps 6-9. Finally, cross reference it using the method described in Steps 11-12.

!!!TEST SERVER!!!

CSAM C&A Web User: Nadine Haddad [Log Out](#) [Tasks](#) [Custom Queries](#) [Help](#)

Home [SSP](#) [Contents](#) [Assessments](#) [POAMs](#) [Reports](#) [Component](#) [Department](#) [Maintenance](#)

**SSP: NOAA5003 - Geostationary Operational Environmental Satellite Ground System** [Comments](#)

[SSP List](#) [General](#) [Info](#) [Types](#) [Locations](#) [Interfaces](#) [Narratives](#) [Appendices](#) [POCs](#) [Artifacts](#) [RTM](#) [Status](#) [Tools](#)

SSP Status						
<a href="#">Edit</a> <a href="#">Refresh</a>	Status:	Initiated	Date Completed	Next Due Date	Expiration Date	Artifacts
Annual Assessment	Completed		4/27/2008	4/27/2009		<a href="#">Q</a>
Certification & Accreditation IAW	ATO		5/30/2008	5/30/2011	5/30/2011	<a href="#">Q</a>
Risk Assessment	Completed		4/27/2008	4/27/2009	4/27/2011	<a href="#">Q</a>
System Security Plan	Completed		3/6/2008	3/6/2009		<a href="#">Q</a>
ST&E	Completed		4/27/2008	4/27/2011		<a href="#">Q</a>
Contingency Plan	Tested		11/19/2008	11/19/2009		<a href="#">Q</a>
Contingency Plan Test			6/25/2008	6/25/2009		
E-Authentication	Not Applicable	0				<a href="#">Q</a>
Privacy Threshold Analysis	Not Started					<a href="#">Q</a>
Personally Identifiable Information	No					
Privacy Impact Assessment	Not Applicable					<a href="#">Q</a>
System of Record Notice ID: NA	Not Applicable					<a href="#">Q</a>
Miscellaneous Artifacts						<a href="#">Q</a>

Configuration Management

Status:	Target Completion:	Completed:	Annual Review:

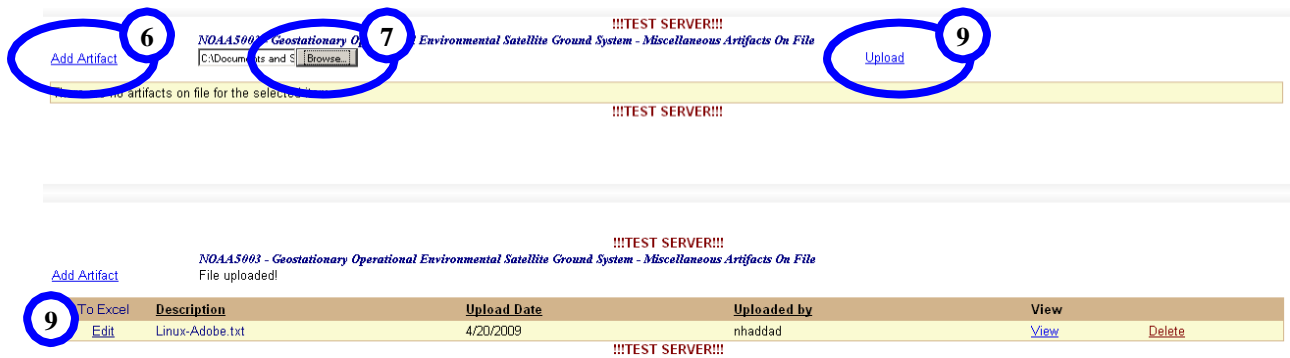
**Step 6.** In the new tab/window, select the "Add Artifact" link.

**Step 7.** In the file field that appears, select "Browse." A File Upload dialogue box will appear.

**Step 8.** Locate the artifact you would like to upload then. Select "Open."

**Step 9.** Select the "Upload" link. The file will now be listed on the current page.

**Step 10.** Close the tab/window.



**Step 11.** Create a cross-reference file using the naming conventions outlined in Table 2 – Naming Convention for Cross-Reference Files which contains a cross-reference and location to the shared artifact (e.g., Please see artifact XYZ in “Miscellaneous Artifacts” located in the NOAA50XX SSP status screen.)

**Step 12.** Upload the cross-reference file using the steps in the next section.

**Table 2 – Naming Convention for Cross-Reference Files**

Label to Include in Filename	Content
XRefP	Includes cross-references to other POA&Ms using the POA&M ID.
XRefE	Includes cross-references to evidence and the location of each in CSAM.
XRef	Contains a list of categorized artifacts and location of each in CSAM.

### 7.5.5.3 Upload an Artifact

To upload a POA&M artifact or file in CSAM:

**Step 1.** In the **POA&M General** tab and next to the “Artifacts” label, select the link “Total.”

**Step 2.** A new window will open.

**Step 3.** In the new window, select the “Add Artifact” link.

**Step 4.** In the file field that appears, select “Browse” and locate the file you would like to upload.

**Step 5.** Select “Open”

**Step 6.** Select the “Upload” link. The file will now be listed on the current page.

### **7.5.6 Identify Closed POA&Ms for Review**

The reports feature in CSAM can be used to identify a sampling of POA&Ms closed in the previous month for the NESDIS CID IV&V.

To conduct a review of closed POA&Ms:

**Step 1.** While in CSAM, select SSP Contents in the top menu.

**Step 2.** In the SSP list, select the SSP for which you would like to download a report.

**Step 3.** Select “Reports” in the top menu.

**Step 4.** Select POA&M.

**Step 5.** Select the field options you prefer.

**Step 6.** Download, save, and open the report on your local system.

**Step 7.** Using the Actual Finish parameter, identify POA&Ms that are closed.

**Step 8.** For each system, select a random 10% of the POA&Ms closed in the previous month.

#### **7.5.6.1 Perform a review**

Perform a review using the method outlined in section 7.5.3.

## 7.6 CSAM Workflow and Approval Status

Those involved in the POA&M process will likely need to update the “Approval Status” throughout the lifecycle of a POA&M. The POA&M approval status is found in the **POA&M General** tab for each POA&M. Figure 6 - Approval Status Field, identifies where the approval status field is located on the **POA&M General** tab.

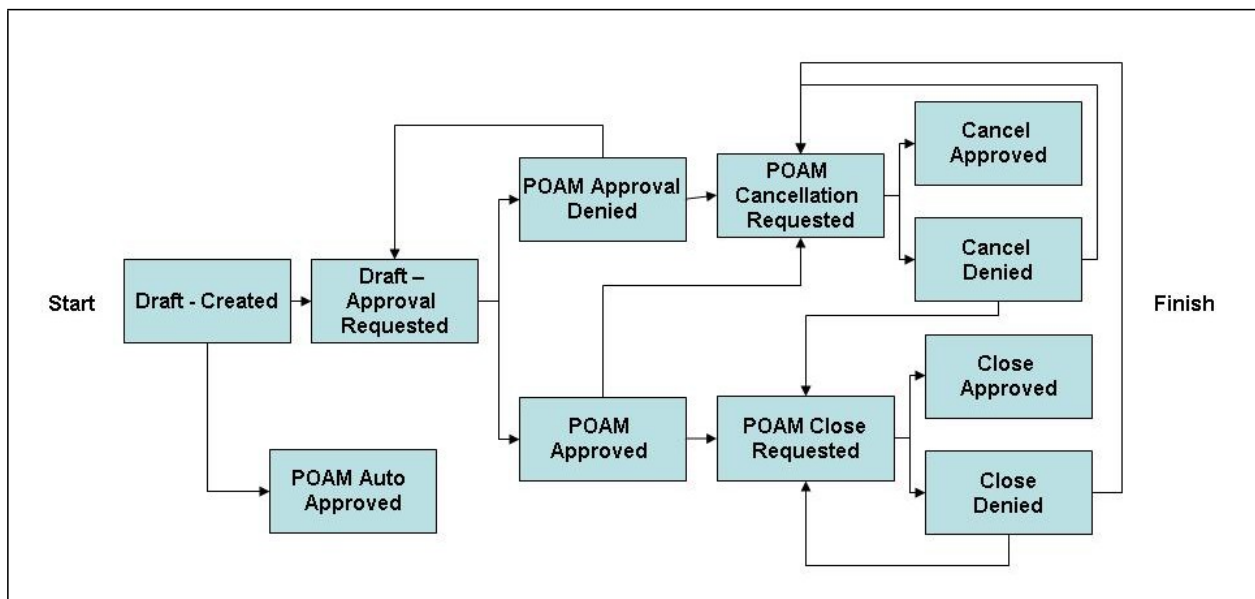
Figure 6 - Approval Status Field

The screenshot displays the 'POA&M GENERAL' tab of a software application. The interface includes the following elements:

- Navigation Tabs:** POA&M GENERAL (selected), Associations, Milestones.
- Header Information:** NOAA5000 - POAM ID: 32131, POAM Seq: 116, POAM Title: [Empty Field].
- Description:** Detailed Weakness Description [Full Screen Edit] (Empty text area).
- Metadata Fields:** Status: Not Started, Severity: no entry, CSAM Derived Criticality, User Identified Criticality: Very Low, Cost: [Empty Field], Assigned: -Select POC-, Assigned Date, Artifacts: Total: 0.
- Checkboxes:**  Weakness,  Exclude from OMB Reporting,  Accepted Risk.
- Scheduling Fields:** Due Date: TBD, Start: TBD, Finish: TBD, Planned: TBD, Actual: TBD, Delay Reason: -No Selection-.
- Action Buttons:** Save, Delete, Cancel, and a highlighted 'Submit' button next to the '-Status Change Request Options-' dropdown.

In many cases an approval status may not occur until another is issued first. Figure 7 – Sequence for Issuing POA&M Approval Status depicts the required sequence for issuing POA&M statuses in CSAM. Table 3 – CSAM Approval Status Summary identifies who issues the approval status, the implications of each approval status, any additional CSAM fields that must be defined before the approval status can be issued (note this does not include POA&M fields required by policy), and the next possible state.

Figure 7 - Sequence for Issuing POA&M Approval Status



**Table 3 – CSAM Approval Status Summary**

<b>State</b>	<b>Additional Required Fields</b>	<b>Issued By</b>	<b>Significance</b>	<b>Next State(s)</b>
Draft - Created	POA&M Title	CSAM	<ul style="list-style-type: none"> <li>• Default status for a newly created POA&amp;M.</li> <li>• POA&amp;M in this state is not considered official or reportable.</li> <li>• POA&amp;M will be auto-approved in 90 days if no action is taken. NESDIS CID has a zero-tolerance policy for auto-approved POA&amp;Ms.</li> </ul>	<ul style="list-style-type: none"> <li>• Draft – Approval Requested</li> <li>• POA&amp;M Auto Approved</li> </ul>
Draft - Approval Requested	<ul style="list-style-type: none"> <li>• POA&amp;M Title</li> <li>• At least one milestone with a description</li> </ul>	SO/ISSO/ SO Designate/ISSO Designate	<ul style="list-style-type: none"> <li>• POA&amp;M is ready for review by ITSO.</li> </ul>	<ul style="list-style-type: none"> <li>• POA&amp;M Approved</li> <li>• POA&amp;M Denied</li> <li>• POA&amp;M Auto Approved</li> </ul>
POA&M Auto Approved	Status comments	CSAM	<ul style="list-style-type: none"> <li>• Occurs automatically after 90 days. NESDIS CID has a zero-tolerance policy for auto-approved POA&amp;Ms.</li> </ul>	<ul style="list-style-type: none"> <li>• POA&amp;M Cancellation Requested</li> <li>• POA&amp;M Close Requested</li> </ul>
POA&M Approved	Status comments	ITSO or Designate	<ul style="list-style-type: none"> <li>• POA&amp;M was approved by the AO(s).</li> <li>• POA&amp;M in this state is considered official and reportable.</li> </ul>	<ul style="list-style-type: none"> <li>• POA&amp;M Cancellation Requested</li> <li>• POA&amp;M Close Requested</li> </ul>
POA&M Approval Denied	Status comments	ITSO or Designate	<ul style="list-style-type: none"> <li>• AO(s) may require changes.</li> <li>• POA&amp;M in this state is not considered official or reportable.</li> </ul>	<ul style="list-style-type: none"> <li>• Draft – Approval Requested</li> <li>• POA&amp;M Auto Approved</li> </ul>
POA&M Cancellation Requested	Status comments	SO/ISSO/ SO Designate/ISSO Designate	<ul style="list-style-type: none"> <li>• Appropriate upon determination that weakness risk should be accepted.</li> <li>• Appropriate if POA&amp;M created in error.</li> </ul>	<ul style="list-style-type: none"> <li>• Cancel Approved</li> <li>• Cancel Denied</li> </ul>

State	Additional Required Fields	Issued By	Significance	Next State(s)
POA&M Close Requested	<ul style="list-style-type: none"> <li>• Status comments</li> <li>• Actual start</li> <li>• Actual finish</li> <li>• Milestone actual finish</li> </ul>	SO/ISSO/ SO Designate/ISSO Designate	<ul style="list-style-type: none"> <li>• All closure requirements have been met.</li> </ul>	<ul style="list-style-type: none"> <li>• Close Approved</li> <li>• Close Denied</li> </ul>
Cancel Approved	Status comments	ITSO or designate	<ul style="list-style-type: none"> <li>• Request for risk acceptance approved by AO(s).</li> <li>• Concurrence that POA&amp;M was created in error.</li> </ul>	None
Cancel Denied	Status comments	ITSO or designate	<ul style="list-style-type: none"> <li>• Request for risk acceptance denied by AO(s).</li> </ul>	<ul style="list-style-type: none"> <li>• POA&amp;M Cancellation Requested</li> <li>• POA&amp;M Close Requested</li> </ul>
Close Approved	Status comments	SO or designate	<ul style="list-style-type: none"> <li>• Closure requirements fully met.</li> </ul>	<ul style="list-style-type: none"> <li>• None</li> </ul>
Close Denied	Status comments	SO or designate	<ul style="list-style-type: none"> <li>• Closure requirements not met.</li> </ul>	<ul style="list-style-type: none"> <li>• POA&amp;M Cancellation Requested</li> <li>• POA&amp;M Close Requested</li> </ul>

### 7.7 POA&M Review Checklist

The following checklist in Table 4 – POA&M Review Checklist is a compilation of guidance from the DOC ITSPP, and the NESDIS CID. The NESDIS CID, SOs, and ISSOs, can use it throughout the various stages of the POA&M process.



**Table 4 – POA&M Review Checklist**

<b>System:</b>	NOAA50XX
<b>Date</b>	mm/dd/yyyy

CSAM Location	Criteria <b>POA&amp;M ID:</b>	12345
POA&M General tab: POA&M Title	POA&M Title concisely describes a weakness (as opposed to a solution or action).	Yes/No
POA&M General tab: POA&M Title or Detailed Weakness Description if there is not enough space.	Identifier that traces back to audit report, SAR, or AO briefing for cross-referencing purposes.	Yes/No
POA&M General tab: Detailed Weakness Description	POA&M description includes enough information to be measurable and observable and support all the reporting and tracking necessary to complete this action. Tip: Check if description indicates <b>what</b> the weakness is. Checked if description indicates <b>why</b> the weakness exists.	Yes/No
POA&M General tab: Detailed Weakness Description	The description of the weakness is virtually the same as the one used in the source document or report, with the exception of sensitive information.	Yes/No
POA&M General tab: Detailed Weakness Description	If sensitive data is included in the POA&M, the POA&M notes the fact of its special sensitivity.	Yes/No/NA
POA&M General tab: Detailed Weakness Description	POA&M Description describes a weak condition (as opposed to a solution or action).	Yes/No
POA&M General tab: Weakness Comments	The source(s) is identified including the name/type of WSR (e.g., Source: Nessus Scan 1/1/2009, or C&A/SAR 6/24/2009)	Yes/No
POA&M General tab: Artifacts	Artifacts are uploaded if necessary to provide additional details of the weakness, including sensitive information (for example, a Vulnerability Assessment Report or scan)	Yes/No
POA&M General tab: User Identified Criticality	The organizational priority is defined according to the associated level of risk and is specified as either High, Medium, or Low as approved by the AO.	Yes/No
POA&M General tab: POC	Select from the drop-down menu the system owner or other responsible party.	Yes/No
POA&M General tab: Cost field	Estimated dollar amount of resources required to resolve the weakness is identified in the cost field. If not yet know, enter "0."	Yes/No
POA&M General tab: Due Date	The POA&M overall scheduled completion date is specified as it was approved by the AO in writing, and it is not earlier than the Planned Finish date.	Yes/No
POA&M General tab: Due Date	The POA&M scheduled completion date represents overall completion of all interim milestones in the POA&M (including AO review, if applicable).	Yes/No
POA&M General tab: Due Date	If the POA&M addresses low or moderate risk, the POA&M schedule allows 15 days before the scheduled completion date for the SO to perform closure review.	Yes/No/NA
Associations tab: Map to Controls	POA&M is associated with a specific NIST SP 800-53 control and the control is identified. Tip: This is important for cross-referencing to the WSR in some cases.	Yes/No
Milestones tab: Milestone	POA&M has at least one milestone.	Yes/No
Milestones tab: Milestone	If the POA&M is high risk, the final milestone is for AO review and concurrence.	Yes/No/NA


CSAM Location	Criteria <b>POA&amp;M ID:</b>	12345
Milestones tab: Milestone	If the POA&M is high risk, the AO review milestone is due no more than 30 days from the completion date of the last SO milestone.	Yes/No/NA
Milestones tab: Milestone	If this is a medium or low risk POA&M, no milestone for AO review and concurrence is included.	Yes/No
Milestones tab: Milestone	Milestone description includes enough information to be measurable and observable and support all the reporting and tracking necessary to complete this action. Tips: Check if milestones describe how the weakness will be resolved. Check if actions described seem to resolve the issue of <b>why</b> the weakness exists.	Yes/No
Milestones tab: Milestone	Each milestone describes a task in the progression of activities toward mitigating the weakness.	Yes/No
Milestones tab: Assigned To	Each individual milestone is assigned to a specific individual(s)	Yes/No
Milestones tab: Due	Each milestone includes a scheduled completion date.	Yes/No
Milestones tab: Planned Start	Each milestone has a planned start date.	Yes/No
Milestones tab: Planned Finish	Each milestone has a planned finish date.	Yes/No
Milestones tab: Milestone and Due	Milestones and due dates overall indicate a reasonable timeframe for mitigating the weakness as approved by the AO. Tips: Expected mitigation timeframes for scan vulnerabilities: -High & critical risk within 30 days -Medium risk within 90 days -Low risk within 120 days Expected mitigation timeframe for other vulnerabilities is within 1 year.	Yes/No
Milestones tab: Milestone	Milestones taken as a whole represent a logical progression to address/mitigate the weakness.	Yes/No
Milestones tab: Milestone and Actual Finish	Actual completion dates for each milestone is provided.	Yes/No
POA&M General tab: Actual Finish	Actual completion for entire POA&M is provided.	Yes/No
POA&M General tab: Artifacts	Artifacts are provided as evidence of POA&M closure and, if necessary, POA&M identification.	Yes/No
POA&M General tab: Artifacts	Artifacts demonstrate that testing for POA&M closure emulates the testing that identified the weakness: Tips: If the source is from vulnerability scanning, an appropriate artifact would be vulnerability scan results showing that a vulnerability no longer exists where it did previously. If source indicates that the weakness was identified through ST&E, SCA, or the SAR, evidence substantiates that NIST 800-53A testing occurred. Artifacts of ST&E or SCA testing would include one or more of the following: -Screen shots of testing -Detailed testing notes -Written policy and/or procedure with applicable approval signatures, where a previous policy and/or procedure did not meet requirements or did not exist -Vulnerability scan results showing that a vulnerability no longer exists	Yes/No

CSAM Location	Criteria POA&M ID:	12345
	where it did previously.	
POA&M General tab: Artifacts	Artifacts substantiate that the weakness was corrected (not planned or partially corrected).	Yes/No
Milestones tab: Milestone and planned Finish	New planned dates for each missed milestone are provided.	Yes/No
POA&M General tab: Delay Reason	If the POA&M is delayed, a delay reason is chosen from the drop-down menu.	Yes/No
POA&M General tab: Delay Comments	If delayed, a narrative comment is provided that elaborates on the delay reason.	Yes/No
POA&M General tab: Artifacts	If AO accepts risk of unmitigated POA&M, AO acceptance is obtained in writing and uploaded as a CSAM artifact.	Yes/No

## Approval Page


Document Number: NQP-3409, Revision 01	
Document Title Block: <b>Plan of Action and Milestones (POA&amp;M) Management Policy and Procedures</b>	
Process Owner: NESDIS ACIO	Document Release Date: September 28, 2012

Prepared by:

  
Erica Boyd  
Ambit- Associate Consultant  
NESDIS Chief Information Office

3/25/15  
Date:

Approved by:

  
Irene Parker  
Assistant Chief Information Officer - Satellites

3/25/15  
Date:

### Document Change Record

VERSION	DATE	CCR #	SECTIONS AFFECTED	DESCRIPTION
2.1	March 25, 2015	----	ALL	Baseline NQP-3409