

Attach 4

United States
Department of the Interior



Plan of Action and Milestones (POA&M)
Process Standard
Version 1.8

May 10, 2010

Document Change History

Version Number	Release Date	Summary of Changes	Section Number/ Paragraph Number	Changes Made By
V1.0	05/04/2005	First release of document.	NA	NA
V2.0	05/13/2005	Bureau comments incorporated.	Various	Alan Wiser
V3.0	09/16/05	Revisions for clarification and to incorporate additional guidance regarding the relationship of POA&MS to Exhibit 300, Process Verification and POA&M Certification.	Various	Carole Dicker
V4.0	10/11/05	Final draft revisions for ITST comment and review.	Various	Larry Ruffin
V5.0	11/8/05	Revisions incorporating ITST comments.	Various	Larry Ruffin Carole Dicker
V6.0	12/5/05	Revisions incorporating additional ITST comments.	Various	Carole Dicker
V1.0	12/19/05	Revisions that incorporate FWS and BLM final comments.	Various	Carole Dicker
V1.1	02/09/06	Revisions that incorporate OSM final comments.	Various	Joe Seger
V1.2	02/09/06	Revisions that incorporate FWS final comments.	Various	Joe Seger
V1.3	12/20/06	Revisions incorporating the ITST's recommendation to add original weakness identification date to the master POA&M template.	Various	Jonas Manalansan
V1.4	01/30/07	Revisions and updates to POA&M reporting template.	Various	Andrea Yates
V1.5	01/28/08	Updated quarterly submission deadlines and points of contact.	Various	Davene Barton
V1.6	2/26/08	Revisions that incorporate ITST comments.	Various	Davene Barton

Department of the Interior POA&M Process Standard

V1.7	3/19/10	<p>The primary revisions incorporate CSAM Version 2.1.3, POA&M management enhancements (Section 4) to include procedures for re-creating POA&Ms that are closed inadvertently, a data field to identify the source of weakness and revisions to the Weakness Completion Verification Form (WCVF).</p> <p>The following documents were added as Appendices: OIG Recommendation Status Reporting Process, CSAM Account Management Procedures and CSAM Rules of Behavior.</p>	Various	Davene Barton and William Ferrell
V1.8	5/10/10	<p>Incorporated changes based on response to the OIG's "Verification of Previous Office of Inspector General Recommendations (Report No. ISD-EV-MOA-0002-2009)"</p>	Various	Larry Ruffin

Table of Contents

1	INTRODUCTION	1
1.1	PURPOSE – ESTABLISH STANDARDS	1
1.2	BACKGROUND	1
1.3	SCOPE	1
2	GENERAL POA&M OVERVIEW	2
2.1	POA&M DEFINITION AND PURPOSE	2
2.2	THE POA&M IN CONTEXT OF CERTIFICATION AND ACCREDITATION	2
2.3	WHICH SYSTEMS REQUIRE A POA&M?	3
2.4	SYSTEM FUNDING AND BUDGETS	3
2.4.1	<i>Funding</i>	3
2.5	BENEFITS OF THE POA&M	4
2.6	ROLES AND RESPONSIBILITIES	5
2.6.1	<i>Departmental Level</i>	5
2.6.1.1	Chief Information Officer is responsible for:	5
2.6.1.2	Chief Information Security Officer is responsible for:	5
2.6.2	<i>Bureau Level</i>	5
2.6.2.1	Authorizing Official is responsible for:	5
2.6.2.2	Authorizing Official Designated Representative is responsible for:	6
2.6.2.3	Bureau Chief Information Security Officer is responsible for:	6
2.6.2.4	Chief Information Officer is responsible for:	7
2.6.2.5	System Owner is responsible for:	7
2.6.2.6	POA&M Coordinator is responsible for:	8
2.7	DEPARTMENTAL OVERSIGHT	8
2.8	HOW TO USE THE POA&M TO PRIORITIZE AND MANAGE REMEDIATION AND RISK	8
2.8.1	<i>Prioritizing Weaknesses for Corrective Action</i>	9
2.8.1.1	System Level Prioritization	9
2.8.1.2	Bureau Level Prioritization	9
2.8.2	<i>Managing and Monitoring Progress</i>	10
2.9	OVERVIEW OF THE POA&M REPORTING CYCLE	11
3	WEAKNESS REMEDIATION PROCESS	13
3.1	IDENTIFYING WEAKNESSES	13
3.1.1	<i>Sources of Weaknesses</i>	13
3.1.2	<i>Including Weaknesses</i>	14

Department of the Interior POA&M Process Standard

3.1.2.1	Program Weaknesses	14
3.1.2.2	System Weaknesses	15
3.1.2.3	Weaknesses Identified Through an Office of Inspector General Evaluation.....	15
3.1.2.4	Weaknesses Identified Through Vulnerability Scanning and Penetration Tests	15
3.1.2.5	Weaknesses Identified Through The Incident Response Management Process	16
3.1.2.6	Weaknesses Identified Through The Internal Control Review Process.....	16
3.2	DETERMINE RISK IMPACT LEVEL.....	16
3.2.1	<i>Weakness Risk Assessment</i>	16
3.2.2	<i>Risk-Based Exceptions</i>	16
3.2.3	<i>Documenting Accepted Risk</i>	17
3.2.3.1	Prior to the system being placed into production:	17
3.2.3.2	After the accredited system is in the operational phase of its lifecycle:	17
3.3	DETERMINING CORRECTIVE ACTION PLAN OPTIONS	18
3.4	DETERMINING FUNDING AVAILABILITY.....	18
3.5	DETERMINING AN ESTIMATED COMPLETION DATE.....	19
3.6	DOCUMENTING THE CORRECTIVE ACTION PLAN IN THE POA&M.....	19
3.7	MONITORING AND REPORTING POA&M ACTIVITY	19
3.8	POA&M WEAKNESS COMPLETION PROCESS.....	19
3.8.1	<i>Corrective Action Completion</i>	20
3.8.2	<i>Independent Verification of Corrective Action Completion</i>	20
3.8.3	<i>Bureau CIO Review of Corrective Action Completion</i>	21
3.8.4	<i>AO's Acknowledgement and Acceptance of Risk(s)</i>	21
3.8.5	<i>Documentation Updates</i>	22
3.8.6	<i>Weakness Completion Follow-Up</i>	22
3.9	POA&M QUARTERLY CERTIFICATION TRANSMITTAL.....	22
4	CREATING AND MANAGING POA&MS	24
5	CONCLUSION	54
	APPENDIX A: REFERENCES	1
	APPENDIX B: ACRONYMS	1
	APPENDIX C: GLOSSARY	1
	APPENDIX D: WEAKNESS COMPLETION VERIFICATION FORM	1
	COMPLETING CORRECTIVE ACTIONS.....	1
	WEAKNESS COMPLETION VERIFICATION FORM.....	2
	APPENDIX E: POA&M CERTIFICATION TRANSMITTAL	3
	APPENDIX F: OFFICE OF INSPECTOR GENERAL RECOMMENDATION STATUS REPORTING PROCESS	1
	APPENDIX G: CSAM ACCOUNT MANAGEMENT PROCEDURES	1

APPENDIX I: CSAM RULES OF BEHAVIOR.....1

List of Figures

Figure 1. Overview of POA&M Reporting11
Figure 2. The POA&M Process for Weakness Remediation.....13

List of Tables

Table 1. POA&M Dates and Deadlines.....11

1 Introduction

1.1 Purpose – Establish Standards

The purpose of the *Plan of Action and Milestones (POA&M) Process Standard* is to provide Department of the Interior (DOI) personnel who have POA&M responsibilities with the standard procedures for developing, maintaining, and reporting their POA&M weaknesses in the Cyber Security Assessment and Management (CSAM) FISMA Reporting solution.

The *POA&M Process Standard* establishes the criteria for the POA&M process to ensure that bureaus and offices effectively implement DOI information technology (IT) security program requirements and that the DOI information security posture and program continues to improve.

1.2 Background

The *DOI POA&M Process Standard* incorporates the POA&M requirements mandated by the Office of Management and Budget (OMB) to comply with the *Federal Information Security Management Act of 2002* (FISMA). The Departmental Office of the Chief Information Officer (OCIO) has integrated the *POA&M Process Standard* into the DOI IT security program to formalize the process of remediating IT Security weaknesses, to ensure that weaknesses are appropriately prioritized for mitigation, and to ensure that all weaknesses are being addressed and resolved.

On April 30, 2007 Interior selected CSAM from the Department of Justice (DOJ), a Shared Services Center (SSC) under the OMB Information Systems Security Line of Business (ISS LOB) to automate FISMA data management and reporting for DOI.

CSAM provides DOI bureaus and offices with automated tools for managing security assessments, developing security plans, and reporting POA&M information. CSAM was purchased as Government Off-the-Shelf (GOTS) software from the DOJ, and during Quarter 4 of Fiscal Year 2008 all DOI bureaus and offices began to use CSAM to manage their FISMA-based information security programs.

1.3 Scope

This document applies to all DOI IT security programs and systems and those individuals having responsibility for:

- Management and operations of IT security programs and systems;
- Ensuring the effective security configuration and posture of systems;
- Identifying, documenting, and implementing corrective actions.

Any personnel tasked with completing POA&M activities should read this document to become familiar with POA&M standards and processes.

2 General POA&M Overview

A POA&M is a management tool that outlines identified IT security program and system weaknesses along with the tasks necessary to correct or mitigate them. To facilitate the remediation of weaknesses, the POA&M provides a means of planning and monitoring corrective actions; identifies those responsible for solving problems; assists in identifying security funding requirements; tracks and prioritizes resources; and informs senior management of the security status of programs and systems.

Remediation of security weaknesses is essential to achieving a mature and sound IT security program. A POA&M process to manage weaknesses is one of the key measures used by the Inspector General (IG), OMB, and Congress to assess an agency's information security program, posture and progress.

2.1 POA&M Definition and Purpose

The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and IT systems. DOI Program Managers are required to use POA&Ms to manage the activities needed to close their security performance gaps, assist the IG in his/her evaluation work of agency security performance, and assist with oversight responsibilities.

The POA&M presents an opportunity to highlight progress and demonstrate improvements in the quality and security of the IT security program. It is also designed to serve as a management tool and as a point of comparison for the OCIO in its assessment of the overall maturity of the DOI's IT security program status.

Though the POA&M is considered a comprehensive plan, OMB operates under the assumption that additional, more detailed project management plans exist for each corrective action item identified in the POA&M. It also assumes that the sources of identified weaknesses (e.g., IG audit reports and risk assessments) are readily available to provide original documentation of each weakness. Thus, each POA&M element should be clearly traceable to any additional project plans and back to its original source(s).

2.2 The POA&M in Context of Certification and Accreditation

According to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 *Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems*, the POA&M is a required document developed during the certification and accreditation (C&A) process and included in the final C&A package to document and help manage the mitigation of weaknesses identified during that process. The POA&M clearly informs the Authorizing Official (AO) of system weaknesses and their associated risks and presents their remediation plans or recommendation to accept the residual risk.

Once the AO authorizes a system for operation, the POA&M becomes part of the continuous monitoring process and is used to document and manage weaknesses identified throughout the system's lifecycle. POA&M weaknesses must be updated in CSAM no less than on a quarterly

basis. The OCIO Cyber Security Division (CSD) is responsible for reviewing and submitting quarterly reports to OMB in accordance with OMB instructions for preparing the FISMA report and Privacy Management report.

2.3 Which Systems Require a POA&M?

All systems that are either in the operational phase of their lifecycle or connected to a production environment potentially affecting other operational systems, or that process live production data require POA&Ms.¹ Below are some special circumstances, and the POA&M requirements they must meet.

- Systems undergoing C&A in preparation for entering a production environment require a POA&M as part of the C&A package. The C&A package POA&M identifies system weaknesses for which corrective actions have been planned and the required funding to implement the changes. New system POA&Ms are created prior to the first C&A phase (Initiation) and are added into CSAM at the time of their creation to ensure complete awareness of upcoming requirements.
- POA&Ms are no longer required for systems once they have been decommissioned.
- Typically, at least one POA&M should be maintained for each system². Separate POA&Ms should not be submitted on minor applications or distributed segments of systems. Exceptions may include such circumstance as when there are instances of an application running locally such as FPPS.

POA&Ms ARE REQUIRED FOR:
<ul style="list-style-type: none">• All systems in production in the operational phase of their lifecycle;• Systems connected to a production environment or processing production data (e.g. pilots); and• Systems undergoing C&A in preparation for production environment.

2.4 System Funding and Budgets

2.4.1 Funding

POA&Ms are used by OMB to assess the state of the Federal Government's IT security and to aid in oversight of the Federal Government and its IT investments. OMB requires tying the POA&M to the budgeting process to ensure funding for IT security costs are considered throughout the system lifecycle. Systems that do not adequately address a plan for securing funding for mitigation of IT security weaknesses can be placed "at risk" and potentially lose funding.

¹ A production system is one that stores, transits or processes live data, or is operating in a production environment. However, please note that if any system meets the described criteria, irrespective of whether or not it is considered to be a production system or in the operational phase of its life cycle (e.g., a pilot or development system either connected to a production environment or that processes production data/information) requires either have an Interim Approval to Operate (IATO) or Authorization to Operate (ATO) and appropriate C&A documentation, including a POA&M.

² A system is defined by the accreditation boundary as documented in the C&A package's System Security Plan (SSP). The inventory of systems must also be maintained in CSAM by each bureau or office and there must be a POA&M corresponding to each of those systems.

For major investments, OMB requires that POA&Ms be cross-referenced through answers to questions when completing section II.B. of the Exhibit 300. The response to all questions in this section of the Exhibit 300 should align with weaknesses reported in the POA&M. Answers to question II.B.1 (A) in the Exhibit 300 (“*What is the total dollar amount allocated to IT security for this investment? Please indicate whether an increase in IT security funding is requested to remedy IT security weaknesses, specifying the amount and a general description of the weakness.*”) should link to each system-level POA&M weakness in the following manner:

- Although the total dollar amount allocated to IT security for the system may not match the POA&M exactly, the Exhibit 300 will include figures from the POA&M in addition to security costs as a separate, but related, component of the ongoing operational and maintenance (O&M) costs.
- The increase in security funding necessary to mitigate the weakness should match those listed in the “Cost” field of the POA&M.
- Identification of the security weaknesses noted in the capital planning document should match those identified in the POA&M.

Bureau or office system owners and Chief Information Officers (CIOs) are responsible for ensuring that the IT security costs necessary to remediate weaknesses are identified, reviewed, and considered in the bureau or office Capital Planning and Investment Control (CPIC) processes, and clearly identified in the POA&M and the Exhibit 300s in a manner that easily distinguishes those costs from routine IT security related O&M costs.

2.5 Benefits of the POA&M

Through the process of strategically addressing vulnerabilities and weaknesses in the POA&M, the mission of DOI can proceed without interruption or failure in appropriate delivery. Beyond its function as the primary authoritative IT security management tool for addressing weaknesses, the POA&M has other benefits related to producing valuable information for trending and analysis, which supports IT business cases, and helps to maintain institutional knowledge and facilitate effective communication among relevant system personnel. Each of these uses provides the OCIO with greater control over its IT security program and increases the efficiency of IT security management.

- **Producing Trending and Analysis Information.** The POA&M can be used as a historical data source for management reporting and business intelligence on the costs, effort, and time to mitigate IT security weaknesses. The type of weaknesses occurring can be tracked, as well as their rate of recurrence. The POA&M provides the ability to conduct analyses by system, program, or across the DOI enterprise.
- **Supporting Business Cases.** A comprehensive POA&M with accurate and reliable financial estimates provides traceability and documents the security funding needed to mitigate weaknesses, specifically at the operational phase of the system lifecycle.
- **Maintaining Institutional Knowledge.** A mature POA&M prevents reliance on one individual to retain and communicate information pertinent to a system or an entire program.

- **Facilitating Effective Communication.** The POA&M facilitates communication and coordination among personnel, such as the CIO, system owners/managers, budget personnel, and program officials.

2.6 Roles and Responsibilities

Within DOI and across the Federal Government, many job roles include POA&M responsibilities. This is because POA&Ms are designed to be used by various types of personnel, including CIOs, Bureau Chief Information Security Officers (BCISOs), the IG, program officials, system owners and system managers, to track the progress of corrective actions for an IT system's weaknesses.

OMB's guidance directs CIOs and program officials to develop, implement, and manage POA&Ms for all programs and systems that they operate and control. For example, for program officials, this includes all systems that support their operations and assets. While much of the focus of security involves IT security professionals, collaboration should also occur with senior management to ensure that weakness mitigation plans are in alignment with the organizational mission and that funding is allocated appropriately. Coordination with budget and program personnel then ensures that weakness mitigation funding is incorporated into capital planning where necessary.

The following DOI role descriptions identify the POA&M responsibilities of each. It is recognized that there may be other individuals with varying titles throughout the bureaus and offices that have been delegated responsibility to fulfill some of the described roles.

2.6.1 Departmental Level

2.6.1.1 Chief Information Officer is responsible for:

- Reporting to OMB on agency progress related to correcting weaknesses reflected in the POA&M and the results of independent IG inspections;
- Reviewing the quarterly POA&M and ensuring that bureaus and offices have followed policies and procedures when completing their respective POA&Ms.

2.6.1.2 Chief Information Security Officer is responsible for:

- Reviewing bureau- and office-level POA&Ms, ensuring that the POA&Ms comply with Department-wide and OMB guidance;
- Implementing a quality assurance process that ensures all systems in the bureau or office system inventory are accounted for, that weaknesses are adequately described, and that planned corrective actions appropriately address the weaknesses.

2.6.2 Bureau Level

2.6.2.1 Authorizing Official is responsible for:

- The quarterly review of systems under their purview prior to the submission of POA&Ms for OMB reporting;
- Reviewing all residual risk(s) recommended for acceptance by the System Owner, User Representative, System Manager, or BCISO.

The Authorizing Official (AO) must either approve or reject each recommendation for risk acceptance. This is an extension of the AO's role of accepting or rejecting risk in the issuance of an authorization to operate (ATO). The AO may delegate activities surrounding the POA&M, but cannot delegate the acceptance of risk to the agency³ and must therefore be the direct approver of any residual risk.

Because of the breadth of organizational responsibilities and significant demands on time, an authorizing official cannot always be expected to participate directly in the planning and technical meetings that occur during the POA&M management process. The AO's designated representative is an individual acting on the authorizing official's behalf in coordinating and carrying out the necessary activities required during the POA&M management and remediation process for an information system.

The AO's designated representative can be empowered by the authorizing official to make certain decisions with regard to the planning and resourcing of the remediation activities associated with weaknesses identified on the POA&M and the determination (but not acceptance) of risk to agency operations, assets, and individuals.

The only activity that cannot be delegated to the AO's designated representative is the acceptance of risk and signing of documents in which the AO indicates acceptance of risk to the agency or IT systems and associated information.

2.6.2.2 Authorizing Official Designated Representative is responsible for:

- Interacting with the BCISO, Information System Owners, System Security Managers, User Representative(s), and other interested parties during the POA&M management and remediation process;
- Reviewing the quarterly POA&Ms and obtain the authorizing official's signature on acceptance of any residual risks when called upon.

If an AO's designated representative is not selected, the AO is responsible for carrying out the activities described above.

2.6.2.3 Bureau Chief Information Security Officer is responsible for:

- Managing the POA&M process to include collection and consolidation of POA&M weaknesses at the bureau level for departmental reporting;
- Ensuring that all OIG recommendations have a corresponding POA&M weakness created in CSAM;
- Communicating standards and procedures related to the POA&M process;
- Reviewing POA&M weakness descriptions to ensure that they adequately describe identified weakness;
- Reviewing corrective actions to ensure that each is an effective and appropriate mitigation solution for its targeted weakness;

³ Refer to NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Page 35.

- Reviewing milestones to ensure that they are relevant and will result in correction or mitigation of each weakness;
- Ensuring that all supporting evidentiary artifacts that support closure of a POA&M weakness has been uploaded into CSAM as an artifact to include, but not limited to, Weakness Completion Verification Forms (WCVFs, screenshots and policy-related documents);
- Reviewing all accepted risk recommendations, ensuring that appropriate justifications are provided and adequately explained;
- Formulating the recommended bureau priority level for identified weaknesses in consultation with System Owners;
- Verifying the completion status of system security weaknesses reported in POA&M;
- Providing routine review and status reports on corrective actions to the bureau CIO, no less than quarterly.

2.6.2.4 Chief Information Officer is responsible for:

- Performing reviews of quarterly POA&M weaknesses and ensuring the accuracy and completeness of the reports;
- Reviewing resource and funding requirements to ensure adequate funding has been identified and committed to implement corrective actions for each weakness;
- Reviewing and reassessing the prioritization of corrective actions;
- Reviewing corrective action verifications to confirm adequate testing and independent review;
- Certifying completed corrective actions in preparation for submission of the FISMA quarterly report, thereby ensuring that completed security weakness remediation activities are documented;
- Ensuring that appropriate program officials have reviewed and accepted any residual risks no less than quarterly.

2.6.2.5 System Owner is responsible for:

- Developing, managing, and implementing POA&Ms;
- Ensuring corrective actions are implemented in a timely manner consistent with the scheduled commitments to resolve weaknesses as documented on their POA&M;
- Preparing documentation for verification of completed POA&M items;
- Completing and uploading Weakness Completion Verification Forms (WCVF) into CSAM as artifacts prior to closing POA&Ms;
- Uploading evidentiary artifacts into CSAM in all updates whether the POA&M remains open or is closed to demonstrate progress in remediating weaknesses;
- Completing and uploading Bureau CIO POA&M Certification Transmittal memoranda into CSAM;

- Updating the C&A package with documentation on completed POA&M items (appendix approved verification form);
- Conducting a routine review and ensuring that updates are entered into CSAM to reflect corrective actions no less than quarterly, in coordination with the BCISO.

2.6.2.6 POA&M Coordinator is responsible for:

The POA&M coordinator is responsible for collecting updated POA&M and or POA&M data from the System Owners or their designees.

- Entering into CSAM POA&M weaknesses and/or updated POA&M weakness information from the System Owners or their designees;
- Ensuring that all supporting evidentiary artifacts that support closure of a POA&M weakness has been uploaded into CSAM as an artifact to include, but not limited to, Weakness Completion Verification Forms (WCVFs, screenshots and policy-related documents);
- Consolidating POA&Ms for quarterly submission to the Cyber Security Division (CSD).

2.7 Departmental Oversight

The Department Manual, part 18, paragraph 18.5(A)1, requires CSD to perform “oversight.” In addition, part 375, chapter 19, paragraph 19.8(D)10, requires the Department’s CISO to oversee “bureau compliance with Federal and Departmental policies, guidelines, and regulations governing IT security.”

The *POA&M Process Standard* establishes the criteria for implementation of DOI’s POA&M process as mandated by OMB. DOI’s OCIO CSD is responsible for ensuring that POA&Ms meet established criteria and are effective in prioritizing and managing weakness remediation and meeting their ultimate purpose of continuously improving the security posture of IT programs and systems throughout DOI. In the event POA&M weakness entries are not in compliance with the *POA&M Process Standard*, the CSD will issue corrective action recommendations to the respective bureau/office POA&M Coordinator.

The CSD will perform annual independent compliance inspections of a sample of completed POA&M corrective actions and will provide reports on the effectiveness of the POA&M processes within each bureau and office.

Each bureau and office should consider the effectiveness of their internal control processes and implement similar verification and validation processes to maintain the integrity of their POA&M and weakness remediation processes. Verification and validation processes should be administered by individuals other than those who are actually responsible for implementing the corrective actions.

2.8 How To Use the POA&M To Prioritize and Manage Remediation and Risk

The POA&M provides a standard format for viewing identified weaknesses and the necessary information to prioritize and manage remediation efforts.

2.8.1 Prioritizing Weaknesses for Corrective Action

FISMA guidance requires Federal agencies to prioritize weaknesses within POA&Ms to help ensure that significant IT security weaknesses within POA&Ms take precedence.

The funding and personnel resources necessary to remediate every weakness identified in the POA&M may not always become available. Therefore, by prioritizing weaknesses in consideration of the varying risk levels associated with each weakness, the bureaus can ensure that critical and high-priority weaknesses receive the funding and personnel resources necessary to complete corrective actions.

The most critical weaknesses for the most critical systems must be considered first. It is not expected, however, that weaknesses will always be resolved in order of severity. Some will require longer-term planning, reallocation of Bureau and Departmental resources, or additional funding. It also often makes sense to resolve the weaknesses that require little effort and use existing funding regardless of priority or weakness severity, assuming the effort does not detract from the more critical issues.

2.8.1.1 System Level Prioritization

At the system level, criteria to be considered in prioritizing weaknesses for corrective action include:

- Risk impact level of weakness (CSAM automatically ranks the criticality of a POA&M when the vulnerability is associated at the Control or Expected Results level. The criticality value is dynamically updated as the associated control implementation status changes);
- Resource (funding and staff) availability;
- Level of effort required to complete corrective action;
- Cost benefit of corrective action (See NIST SP 800-30 for recommendations in performing cost-benefit analysis);
- Length of time since the weakness was identified;
- The AO's tolerance for the duration of risk exposure;
- Circumstances unique to the system.

Program officials and System Owners in consultation with the BCISOs should use their best judgment in consideration of the above factors and incorporate the urgency for corrective actions into their project plans.

2.8.1.2 Bureau Level Prioritization

At the bureau level, prioritizing weaknesses for corrective action is necessary for an effective allocation and/or reallocation of funds. Prioritizing weaknesses for corrective action is more complicated than it is at the system level, as the decision must consider all of the bureau's systems. The following factors should be considered at the bureau level:

The security categorization of the system as defined by the NIST Federal Information Processing Standard (FIPS) Publication (Pub) 199⁴ and the associated potential impact ratings for confidentiality, integrity, and availability. This is documented in each system's System Security Plan (SSP). Prioritization of corrective actions should be based on the most critical and sensitive systems first;

- The risk impact level of each weakness within a system's POA&M;
- Potential corrective action cost;
- Cost/benefit of corrective action;
- Potential for funding reallocation;
- Extent of the system's overall non-compliance.

Although a formal cost/benefit analysis is not required, for large systems with potentially costly corrective requirements, good project management may call for a cost benefit analysis to determine the best solution and acceptable level of residual risk.

2.8.2 Managing and Monitoring Progress

The POA&M is intended to serve as a tool for managing the progress of corrective actions and thereby managing risk posed by the weaknesses. At all levels—system, bureau, OIG, Departmental—the POA&M provides a view of progress within each system, for the system as a whole, and on a bureau-wide level.

Individual POA&Ms should be reviewed regularly to determine whether there are unnecessary delays, if priorities have shifted in light of newly identified weaknesses or environmental changes, and whether resources need to be re-evaluated. At the bureau level, the System Owner and BCISO are tasked with this responsibility, but it is also within the purview of the CIO to provide oversight. From a wider perspective, common weaknesses across the bureau or agency can be detected and more effectively dealt with, or areas requiring additional attention can be identified.

The quarterly reporting schedule for bureaus and offices to have POA&M updates entered into CSAM is depicted in the table below. Please note that if the due date falls on a Saturday or Sunday the updates are due the following Monday by close of business.

⁴ System security categorization should be determined according to the criteria articulated in the Federal Information Processing Standards (FIPS) Publication 199, *Security Categorization of Federal Information and Information Systems* and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems*.

Quarter	Time Period Covered	Deadline for bureaus and offices to have updates entered into CSAM	Deadline for CSD Submission of Report to OMB
1st	Aug 1 - Oct 31	November 6	December 1
2nd	Nov 1 - Jan 31	February 6	March 1
3rd	Feb 1 - Apr 30	May 6	June 1
4th	May 1 - Jul 31	August 6	September 1

Table 1. POA&M Dates and Deadlines

In summary, the POA&M provides a means to monitor corrective actions, to ensure flexibility as the environment changes, to maintain a focus on priorities, and to minimize delays. It facilitates the decision-making process with regard to budget formulation and resource allocation or re-allocation. The POA&M is also a means to demonstrate compliance with policy and to show progress toward an improved security posture.

2.9 Overview of the POA&M Reporting Cycle

OMB POA&M reports consist of summary information on identified weaknesses, which are tracked in the agency's program and system POA&Ms. POA&M reports that are broken down by major agency components--DOI bureaus and offices--must be submitted quarterly to OMB.

DOI bureaus and offices are the source of this information, and must therefore provide the DOI CSD with up-to-date POA&M packages via CSAM on a quarterly basis. The DOI CSD program office then reviews and consolidates the information and presents the quarterly report to the Departmental CIO. The Departmental CIO reviews and approves the report and forwards it on to OMB.

The quarterly POA&Ms provide OMB with a 'snapshot in time' of the ongoing activity directed toward improving DOI's overall IT security posture.

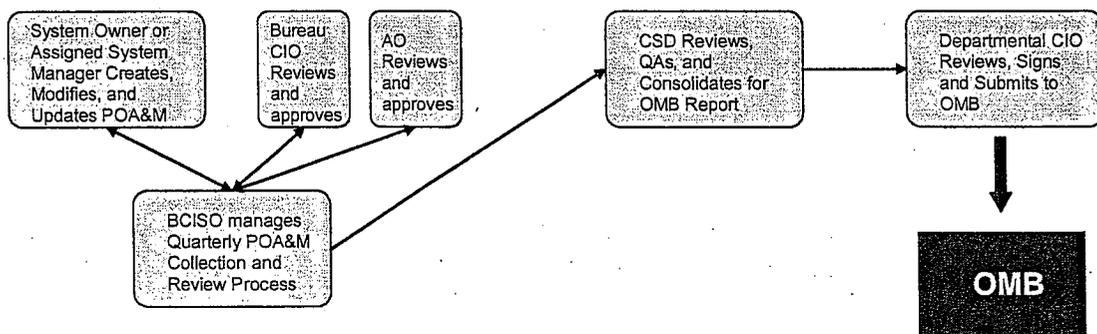


Figure 1. Overview of POA&M Reporting

Bureaus and offices should establish their own internal deadlines consistent with the time period covered and CSD's deadline for POA&M package submission to OMB. In order to meet the

regularly occurring deadlines, it is recommended that System Owners—or individuals delegated the POA&M responsibility—integrate the POA&M process into a continuous monitoring process. This will allow for sufficient time to gather information, make certain decisions, and obtain necessary AO and CIO quarterly review and approval. Each bureau or office POA&M update must include:

- **Updated POA&M for each system** in the bureau or office inventory and the bureau or office IT security program. (See Section 2.3, *Which systems require a POA&M?*) For each system and program the POA&M weakness must be updated in CSAM no less than quarterly to include updates to all relevant date fields as well as key milestones.

The key milestones associated with each corrective action should be identified on each POA&M. Each weakness must have one or more associated milestones. Milestones should define the major steps that will be performed to complete the corrective action. If there is more than one milestone, enter the milestone in the order they should be executed. For example, one set of milestones for a weakness such as, "Identification and authentication are not adequate for the level of security controls required for this system" might be:

- 1) Evaluate methods for strengthening identification and authentication.
- 2) Recommend solution and obtain approval.
- 3) Develop procedures to standardize accepted identification and authentication process.
- 4) Design identification and authentication solution.
- 5) Build identification and authentication solution.
- 6) Test identification and authentication solution.
- 7) Deploy identification and authentication solution and implement supporting process.

Milestones might also include more specific aspects related to the technical solution (e.g. implement two-factor authentication), and management and operational controls related to the steps for implementing supporting business practices and procedures where additional security control requirements are known or anticipated.

The description of each milestone must be detailed enough so that an independent reviewer will understand the planned corrective action and determine whether the corrective action is adequate and appropriate and will result in the weakness being corrected or its associated risk mitigated to a level acceptable to the AO. The last milestone entry must clearly identify the action taken to mitigate the weakness. Sensitive information can be included as needed for the description since the entire POA&M is a sensitive but unclassified document.

A copy of the WCVF for each system which will be uploaded as an artifact into CSAM. Each completed weakness requires a form, signed by the System Owner, an Independent Reviewer, Lead Responder, the CIO, and the AO if there is any residual risk. (See Appendix D, *Weakness Completion Verification Form*.)

- **POA&M Certification Transmittals**, signed by the bureau or office CIO covering all systems within his or her respective bureau or office. The transmittal certifies that the POA&Ms were completed in accordance with DOI OCIO Directive 2006-007. The CIO Certification Transmittal must list each system in the bureau or office inventory, its

operational status (pre-production, production, or decommissioned), and its C&A status (ATO, IATO, no authorization to operate). (See Appendix E, *POA&M Certification Transmittal*.)

Attached to each CIO Certification Transmittal are the **AO Certification Transmittals** indicating review of the POA&Ms for the systems for which each AO is responsible. (See Appendix E, *POA&M Certification Transmittal*.)

3 Weakness Remediation Process

Weakness remediation consists of a cycle that entails the steps depicted in Figure 2 below.

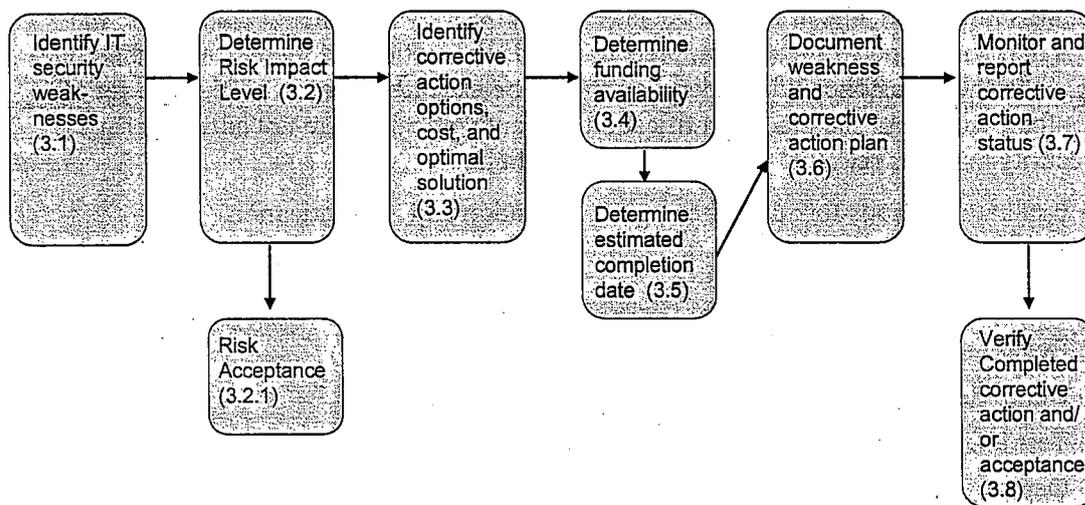


Figure 2. The POA&M Process for Weakness Remediation

This section describes the Weakness Remediation Process for implementing the steps in this process, including the identification, documentation, and updating of weakness information in the POA&M. Section 4 provides instructions for recording all required information into CSAM, including a field-by-field description of the POA&M contents.

3.1 Identifying Weaknesses

Weaknesses to be recorded and tracked through the POA&M process can be identified through either reactive or proactive processes. Reactive weakness determination indicates that outside auditors or reviewers identified the weakness. Proactive weakness determination occurs by conducting regular program and system reviews using various internal assessments.

3.1.1 Sources of Weaknesses

A DOI-specific User Defined Attribute (UDA) labeled “Source of Weakness” has been created within CSAM and is now an attribute of every POA&M weakness. This is in addition to the existing DOI-specific UDA labeled as “Created as a Result of an OIG Evaluation” having a value of either “Yes” or “No” that will continue to be maintained to enable the OIG to more efficiently identify all POA&M weaknesses that are associated with OIG report findings and

recommendations. The new "Source of Weakness" UDA provides a text field with a sufficient number and types of permissible characters for bureaus/offices to identify all sources of weaknesses by including the auditing entity, the title of the report, the report number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness.

Typical sources of identified weaknesses that must be added to the POA&M include, but are not limited to, the following:

- OIG audits and reviews
- OCIO - FISMA activities
- Annual self-assessments
- GAO reviews
- Court ordered reviews
- OMB activities
- Third party audits
- Risk assessments
- Penetration tests
- Vulnerability scans
- Day-to-day operations

Bureaus/Offices must enter the source of each weakness and must include the title of the report, the report number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness.

3.1.2 Including Weaknesses

POA&Ms must include all security weaknesses, not just material or reportable weaknesses, associated with DOI systems and programs. Weaknesses that can be corrected in a short time frame or are considered low risk and acceptable must still be included in the POA&M and tracked until verified as complete. The POA&M is the authoritative DOI-wide management tool and, as such, should represent an all-inclusive view of identified security weaknesses. The two types of weaknesses, program and system, are described below.

3.1.2.1 Program Weaknesses

A program weakness impacts multiple IT systems as a result of a deficiency in the IT security program. Program weaknesses are generally weaknesses that affect the bureau or office as a whole. Program weaknesses are addressed separately from individual system weaknesses. An example of a program weakness is: "Security policy is not updated with latest legislative guidance."

3.1.2.2 System Weaknesses

A system weakness pertains to the management, operational, or technical security controls of a specific IT system. Each set of system-specific weaknesses is noted under separate headers in a POA&M. An example of a system weakness is: "System has not been certified and accredited/authorized to operate."

3.1.2.3 Weaknesses Identified Through an Office of Inspector General Evaluation

All weaknesses identified as a result of an OIG evaluation should have a single unique POA&M weakness created for each individual recommendation within three business days of receiving the report. (See Appendix F, *Office of Inspector General Recommendation Status Reporting Process*.) In other words, there should only be a single POA&M item per OIG recommendation, even if the corrective action for each appear to be the same. This requirement stems from a previous OIG finding and recommendation and currently only applies to OIG recommendations.

3.1.2.4 Weaknesses Identified Through Vulnerability Scanning and Penetration Tests

Weaknesses may be identified during routine vulnerability scanning (e.g., weekly or monthly) in support of the continuous monitoring process. These vulnerabilities should be validated and the POA&M weakness must be created in CSAM. It is recognized that there may be false positives and that a number of weaknesses may be immediately resolved. There are also varying levels of risk for the vulnerabilities identified in the scans. The following discussion addresses guidelines regarding pre-POA&M evaluation.

Pre-POA&M Evaluation and Corrective Action –The following guidelines should be used to prioritize, evaluate, and validate the scanning results.

- High-risk or critical vulnerabilities associated with internet-accessible and/or externally facing systems have a period of up to ten (10) calendar days prior to recording weaknesses as a POA&M in CSAM. (Note, however, that such vulnerabilities are typically associated with any attacker being able to exploit a weakness remotely without requiring elevated/privileged access to a system and should be addressed immediately by disabling any access to the vulnerable service until the risk can be mitigated to at least a medium level before restoring the service);
- Medium-risk vulnerabilities associated with internet-accessible and/or externally facing systems have a period of up to thirty (30) calendar days prior to recording weaknesses in a POA&M;
- Low-risk vulnerabilities associated with internet-accessible and/or externally facing systems have a period of up to sixty (60) calendar days prior to recording weaknesses in a POA&M;
- High-risk vulnerabilities associated with internal systems (that are NOT internet-accessible and/or externally facing) have a period of up to fifteen (15) calendar days prior to recording weaknesses in a POA&M;
- Medium-risk vulnerabilities associated with internal systems (that are NOT internet-accessible and/or externally facing) have a period of up to thirty (30) calendar days prior to recording weaknesses in a POA&M;

- Low-risk vulnerabilities associated with internal systems (that are NOT internet-accessible and/or externally facing) have a period of up to sixty (60) calendar days prior to recording weaknesses in a POA&M.

Aggregating Scan Identified Vulnerabilities Into Individual POA&Ms – Multiple vulnerabilities from a vulnerability scan or any other source cannot be recorded as a single POA&M weakness entry. Each vulnerability or weakness identified should be verified and an individual POA&M weakness must be created for each weakness. The source of the weakness must be identified in the “POA&M Title” field within CSAM.

3.1.2.5 Weaknesses Identified Through The Incident Response Management Process

Weaknesses identified through the Incident Response Management Process should typically be included in a POA&M. However, if remediation is completed immediately as part of the incident response, if the DOI-CIRC incident report sufficiently documents the corrective action, and if the corrective action fully addresses the weakness (e.g., there is no resulting residual risk), then it is not necessary to report it as a POA&M or in an existing POA&M. A POA&M entry is required if corrective action is not completed within five (5) calendar days.

3.1.2.6 Weaknesses Identified Through The Internal Control Review Process

Weaknesses identified through the Internal Control Review (ICR) process must be entered into CSAM as part of the documentation process. A copy of the POA&M is **not** required as part of the ICR submission. A POA&M weakness must be created in CSAM with identified corrective measures necessary to bring each security control into full compliance, unless a prior POA&M weakness was created and the risk has been accepted or compensating controls are in place.

Bureaus and offices must submit within their assurance statements, as part of their normal POA&M reporting process, all weaknesses that note a deficiency of security controls for their information systems. POA&M submissions of the weaknesses identified during the ICR process are required regardless of whether their conditions rise to the level of being “reportable.”

3.2 Determine Risk Impact Level

3.2.1 Weakness Risk Assessment

CSAM automatically ranks the criticality of a POA&M when the vulnerability is associated at the Control or Expected Results level. The Criticality value is dynamically updated as the associated control implementation status changes.

3.2.2 Risk-Based Exceptions

In some cases, a specific corrective action may not exist for a weakness because the weakness is considered an acceptable risk. The weakness must still be recorded in the POA&M to document the decision in the quarter in which it was discovered and must continue to be reported until the risk is formally accepted by the AO. The AO is the only official that has the authority to accept the residual risk from a partially or un-remediated weakness.

The AO acknowledges and accepts the risk when he or she completes the quarterly review of the POA&M containing the documented weakness. At a minimum, the CIO, System Owner, System Manager and/or BCISO should provide the AO with a quarterly briefing of the information

necessary for the AO to make an informed, risk-based decision regarding the POA&M-defined milestones with respect to accepting the existing residual risks.

All high-risk weaknesses must be corrected if possible or otherwise mitigated to at least a medium level of risk. (The AO can only consider acceptance of medium or low risks) Every effort must be made to correct or further mitigate all risks to a level commensurate with the potential impact to systems and associated data.

3.2.3 Documenting Accepted Risk

Using the WCVF (Appendix D), and complying with an approved procedure to assess risk such as that identified in NIST 800-30, *Risk Management Guide for Information Technology* the System Owner or designated individual should record the rationale and justification for risk acceptance to facilitate the AO's decision-making process. The System Owner should take measures to fully understand and document the level of risk and possible compensating controls. Measures such as researching the risk and evaluating industry common best practices for remediation strategies will show the System Owners prudent judgment and due diligence. Because risks can change over time, the System Owner should also periodically review the system's accepted risks to assess any potential changes in the acceptable risk level. Details on the process and documentation for acceptance of risks are further discussed in Section 3.8, *POA&M Weakness Completion Process*.

The AO's risk acceptance must also be appropriately documented. The following scenarios are acceptable forms of documenting risk acceptance decisions. Rationales and justifications must be included in the documentation.

3.2.3.1 Prior to the system being placed into production:

At the time the AO issues an ATO for a specific system, risks to be accepted by the AO can be documented in either the:

- The AO's Accreditation Memorandum;
- The Certifying Official's Certification Statement with a reference in the AO's Accreditation Memorandum stating that the risks identified in the Certification Statement are to be accepted; or
- The SSP with a statement in the AO's Accreditation Memorandum stating that the risks identified in the SSP are to be accepted.

The Accreditation Memorandum should also include an explicit statement that the AO acknowledges and accepts those risks, including any specific duration for or terms and conditions on which the risk acceptance is based.

3.2.3.2 After the accredited system is in the operational phase of its lifecycle:

New residual risks identified after C&A activities have been completed must also be accepted by the AO. This can be accomplished by revising the SSP and updating the Risk Assessment Report (RAR). Appending the WCVFs signed by the CIO and the AO (when residual risk exits) will serve this purpose, until these documents undergo formal revision.

The milestone for the corresponding weakness must be included in the POA&M (e.g., “AO Risk Acceptance requires updates to the SSP and RAR to document the AO’s risk acceptance decision, terms, duration, and conditions, and any additional required management, operational, or technical security controls to be implemented”).

For scenarios that require additional controls to be implemented in order to mitigate the risk to a level acceptable for the AO, those milestones must also be included with details validating their completion.

3.3 Determining Corrective Action Plan Options

There are often multiple methods of remediating a weakness. Various methods should be analyzed to determine the most appropriate corrective action for resolving the weakness and with respect to long-term implications. The system category combined with the security control guidance in *FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems* and the associated *NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and the DOI IT Security Policy Handbook, Version 3.1, March 18, 2008*, are basic factors in the selection of mitigation alternatives. NIST SP 800-53 Revision 3, specifies minimum security controls for systems based on each system’s overall security categorization and potential impact ratings (e.g., high, medium, and low) for confidentiality, integrity, and availability. In addition, the cost for each corrective action plan option must be estimated and analyzed to determine short-term and long-term solution capabilities.

The corrective action plan must be well thought out and specifically address the issue it is intended to resolve. A corrective action plan may fully correct a weakness or, alternatively, partially mitigate the weakness to reduce the risk to a level acceptable by the AO. In certain situations, there will be no corrective action planned and risk acceptance will be proposed. (See Section 3.2.2, *Risk-Based Exceptions*)

3.4 Determining Funding Availability

Funding for corrective actions can be obtained through the following means:

- Using current funding marked for security management of the system or program;
- Reallocating existing funds or personnel; or
- Requesting additional funding following the department’s and bureau’s budget process.

If new funding is required, it is imperative that the department’s and bureau’s capital planning process is correctly followed to obtain the necessary funds. While the Department requires the reporting of POA&M security costs, which are then reviewed at the department level, the expectation is that the vast majority of remediation costs are to be addressed by each investment’s existing base funding or through re-planning of funding from other investment budgets. A medium- or high-risk weakness typically requires immediate attention and cannot wait for a future budget cycle.

Integrating IT security costs with the capital planning process ensures that security is included in the agency's enterprise architecture, supports business operations, and is funded within each information system over its lifecycle.

3.5 Determining an Estimated Completion Date

The estimated date of completion for each corrective action should be based on the outcome of prioritization decisions and in consideration of resource utilization. However, prioritization is not necessarily aligned with completion dates.

Timelines should be realistic and consider all steps and funding needs involved in the level of effort required to correct a weakness. Although several weaknesses may each take 30 days to complete individually, it may not be possible to complete numerous weaknesses during a 30-day period if the same staffing resources are involved. Also, if the corrective action is a long-term solution requiring multi-year funding, then the milestones and completion date should reflect these factors.

3.6 Documenting the Corrective Action Plan in the POA&M

OMB established the foundational structure of the POA&M to provide consistency in the collection and presentation of information. The POA&M module in CSAM was created based upon OMB's POA&M structure. (See Section 4, *Creating and Managing POA&Ms*.)

3.7 Monitoring and Reporting POA&M Activity

The POA&M should be maintained regularly by the System Owner or designee by amending them with newly identified information and updating the status in the comment field of already documented weaknesses as they go through the mitigation process. In addition, corrective actions must be monitored for progress delays, effectiveness, and changes in risk level. Although quarterly POA&Ms provide OMB with a 'snapshot in time' of ongoing activity directed toward improving the overall security posture of DOI's IT environment, ongoing progress monitoring of planned activities is a best practice for any project plan.

3.8 POA&M Weakness Completion Process

FISMA guidance states that the "Completed" status for a weakness should be used only when a weakness has been fully resolved and the corrective action has been tested. Remediation actions must be specific to the weakness identified and ensure slight to no risk of recurrence of the same weakness. Should the weakness recur, there should be compensating controls in place to detect the weakness.

To 'close' a POA&M weakness and consider remediation activity complete, the POA&M must be properly completed and populated in CSAM in accordance with the guidance in this document. The WCVF in Appendix D must be completed and uploaded into CSAM as an artifact as well as evidentiary artifacts that support closure of the POA&M weakness. The WCVF documents all activities and justifications, which must be approved in writing with all required signatures, for closure of all reported weaknesses. This includes corrective action that results in complete remediation or partial remediation with residual risk, or when no corrective

action is taken, which also results in residual risk. In the case of residual risk, the WCVF documents the AO's decision to accept the residual risk.

The WCVF is applicable to weaknesses identified in both the system and program POA&Ms. Copies of these forms become part of the quarterly POA&M package submission and must also be maintained as part of the C&A package documentation for each system to update the SSP and the Risk Assessment Report.

The WCVF is not required for systems that have been officially decommissioned. The decommissioning memorandum must be uploaded into CSAM prior to closing the POA&M weakness.

The following sections outline the process to complete the WCVF required to move a POA&M weakness to a 'completed' status.

3.8.1 Corrective Action Completion

The System Owner (or designee) must review the evidentiary documentation of the completed weakness remediation. Any corrective action must have followed a structured process of implementation, testing, and documentation. Some examples of sources of information that *demonstrate* resolution of a security weakness include, but are not limited to: change control logs (signed/dated/verified or reviewed); test report results related to system changes; contingency/continuity of operations test reports; contingency plan testing with documented results of table top exercises; hard-copy user access control/review lists (signed/dated); contingency plans/tests (signed/dated).

The System Owner must also evaluate the risk-impact level of any residual risk. In cases where no corrective action is taken, the System Owner must document the rationale and justification for risk acceptance. Similarly, in cases where the corrective action for a high-level risk results in only partial mitigation and the residual risk level is subsequently reported as medium or low, the System Owner must document the rationale and justification as to why he or she now considers the reported weakness risk level to be less than high.

The System Owner then completes and signs off on the WCVF, Part I attesting to the implementation of the corrective action and update the milestones in CSAM accordingly.

3.8.2 Independent Verification of Corrective Action Completion

Corrective actions must be independently verified and tested to ensure that remediation efforts affect the intended results and adequately address the security weakness. This process also verifies that remediating controls are in place and that any other known remaining residual risks have been identified.

The independent reviewer should not be an individual who plays an active role in managing the system under review as this is considered a conflict of interest and may hinder a truly independent evaluation of documentation or technical solutions. The Regional Information Security Officer (RISO) or BCISO are individuals who can fill the role of independent reviewer, but the role is not limited to these personnel. It is up to the bureau or office to designate

appropriate independent reviewers. However, POA&Ms created as a result of an OIG evaluation must remain open until the Cyber Security Division (CSD) POA&M and Audit Liaison Service Area has the opportunity to re-evaluate them and confirms they are resolved to their satisfaction (See Appendix F, *OIG Recommendation Audit Reporting Process*).

The independent reviewer will review documents compiled by system teams or perform other testing as necessary to ensure that technical solutions implemented as the corrective action are working as intended and satisfactorily address the identified weakness. The review process may include 'shoulder surfing' or visual inspections of technical solutions, documentation reviews, and inspections and evaluations of technical tests results. The independent reviewer must document the assessment method and his or her findings and sign the WCVF, Part II.

3.8.3 Bureau CIO Review of Corrective Action Completion

Bureau CIOs are responsible for reviewing and approving all completed corrective actions. The CIO has the option of rejecting the 'Completed' status of system security weaknesses. If this occurs, the previously completed or accepted weakness will be returned to the system or project team and the POA&M weakness will be re-created in CSAM with a revised corrective action plan. The re-created (new) POA&M **must** reference the original POA&M ID number in the "POA&M Title" field. Additionally, the original (old) POA&M **must** reference the re-created POA&M ID number in the "POA&M Title" field.

Bureau CIOs will review the WCVF and other evidentiary documentation as needed to evaluate a completed system security weakness and verify that internal controls associated with the POA&M reporting process are working as required. CIOs must sign the WCVF, Part IV, attesting to the fact that corrective actions have been implemented correctly prior to closing the weakness in the POA&M.

3.8.4 AO's Acknowledgement and Acceptance of Risk(s)

The AO is responsible for thoroughly reviewing all residual risk recommended for acceptance by CIOs, System Owners, System Security Managers, or BCISOs. The AO can either approve or reject the recommendation. If the AO chooses to reject the recommendation, then the POA&M weakness must be re-created in CSAM and a revised corrective action plan must be prepared. This is an extension of the AO's role of accepting or rejecting risk in the issuance of an ATO.

In accordance with the *Information Technology Security Policy Handbook*, in considering whether or not to accept the risks indefinitely or for some specified time, the risk acceptance documentation must identify any conditions and constraints under which those risks will be accepted by the cognizant AO (e.g., specified acceptable duration within which the AO will tolerate continued acceptance of the risk, any required mitigating actions and/or compensating controls to be implemented as interim protective measures, etc.) Where the AO is unwilling to accept risks indefinitely, the weakness must be incorporated into the appropriate program- or system-level POA&M. These are the appropriate means, and only formal methods available, that are consistent with FISMA, OMB, and NIST standards and guidelines by which weaknesses are effectively understood, documented, accepted, managed, and tracked. There are no provisions to request any other form of exemption to policies and standards.

To consider the remediation complete, the AO must acknowledge the residual risk of each completed corrective action and indicate his or her acceptance by signing the WCVF, Part V. If a corrective action fully mitigates all risk, then it is not necessary for the AO to review the WCVF.

In order for the AO to fulfill this responsibility, the CIO, System Owner, BCISO or AO's designated representative should provide quarterly briefings to the AO to facilitate the risk acceptance process.

All high-risk weaknesses must be corrected if possible or otherwise mitigated to at least a medium level of risk. The AO can only consider acceptance of medium or low risks. When economically feasible, every effort must be made to correct or further mitigate all risks to a level commensurate with the potential impact to systems and associated data.

The AO is the **only** official authorized to accept security risks for the systems under his or her purview and they must document their acceptance of those risks.

3.8.5 Documentation Updates

When identifying weaknesses, completing corrective actions, or accepting risk, in addition to the POA&M, other documentation must be regularly updated.

- **System Security Plan** – The SSP must be updated when controls are changed or added to a system as part of a corrective action plan. Also, the formal acceptance of risk in a required control category should be documented in the SSP. Until the SSP is formally revised, however, appending the WCVF and supporting documentation to the SSP will satisfy this requirement.
- **Risk Assessment Report** – The Risk Assessment Report must also be updated if there is long-term residual or accepted risk. Appending the WCVF and supporting documentation to the Risk Assessment Report will satisfy this requirement.

3.8.6 Weakness Completion Follow-Up

Periodically, or at least quarterly, all residual and accepted risks associated with a weaknesses should be reviewed to determine whether changes in architecture, security controls, technology, exposure (e.g., to the Internet or other internal/external system interconnections), information sensitivity, or business practices have altered security risks for the system. If overall risks (risks at the aggregate level) have increased, the responsible officials should take appropriate measures, including adding a new system weakness to the POA&M. All risk related actions and periodic reviews must be updated in the POA&M milestones accordingly.

3.9 POA&M Quarterly Certification Transmittal

The Certification Transmittal requires that bureau CIOs review all aspects of their organizations' program and system POA&Ms for the current quarterly submission. The objective is to ensure that the POA&Ms are completed in accordance with the standards described within this *POA&M Process Standard* as per DOI OCIO Directive 2006-007.

The Certification Transmittal also requires that each AO within the bureau or office review all aspects of the system POA&Ms for which he or she is responsible. The intent is to ensure that the AOs have been briefed on and understand the current security status of the systems for which they are responsible. This covers the risks relating to the current set of unmitigated weaknesses, not just the risks that they have formally accepted as part of the C&A process and the POA&M weakness completion process. Because there may be more than one AO within a bureau or office, the Certification Transmittal is divided into two sections. A Certification Transmittal from the CIO and a separate Certification Transmittal from each AO.

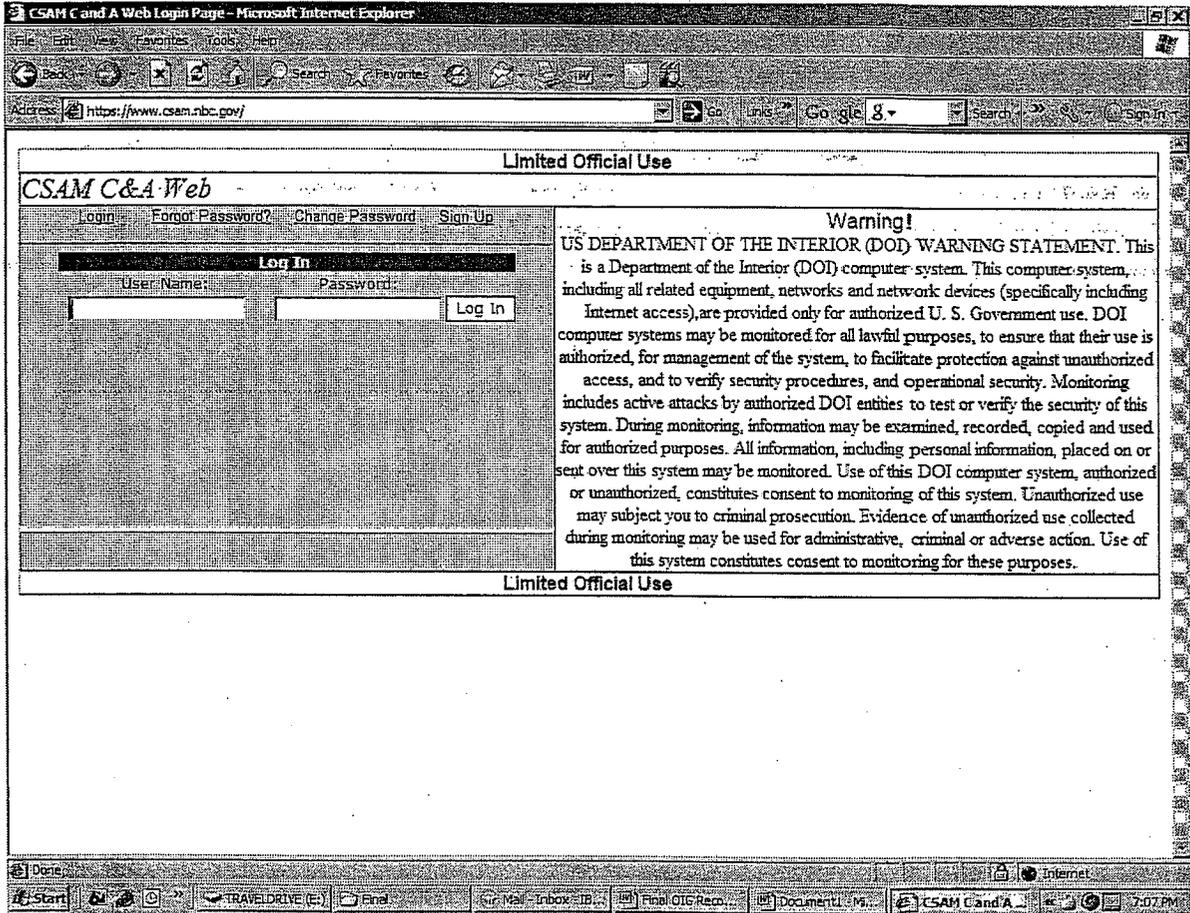
CIO Certification Transmittal – The bureau CIO will review the quarterly POA&M packages submitted by each of the bureaus and provide a signed Certification Transmittal covering all systems, certifying the POA&Ms compliance and acceptability. The quarterly Certification Transmittal must list all of the systems for that bureau or office, their operational status, and their C&A status. (See Appendix E, *POA&M Certification Transmittal*) The AO Transmittals are appended to the CIO Certification Transmittal.

AO Certification Transmittal - AOs will review the POA&Ms for systems they are responsible for and provide a signed Certification Transmittal attesting to their acceptance of the security posture of the system. (See Appendix E, *POA&M Certification Transmittal*.)

4. Creating and Managing POA&Ms

This section will explain how to create and manage program and system POA&Ms in CSAM. Please refer to Appendix F, *Office of Inspector General Recommendation Status Reporting Process*, for guidance on POA&M weaknesses that are created as a result of an OIG evaluation.

1. To create a program or system POA&M go to: <https://www.csam.nbc.gov>.
2. Enter your User Name and Password and then select **Log in**.



3. Select the POA&Ms link.

CSAM C&A Web Home - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <https://www.csamtest.nbc.gov/CSAMCentral.aspx> Go Links Google Search Sign In

TEST SERVER - Limited Official Use - TEST SERVER

CSAM C&A Web User: Davene Barton Log Out Tasks Custom Queries Help

Home SSP Contents POAMs Component Department Maintenance

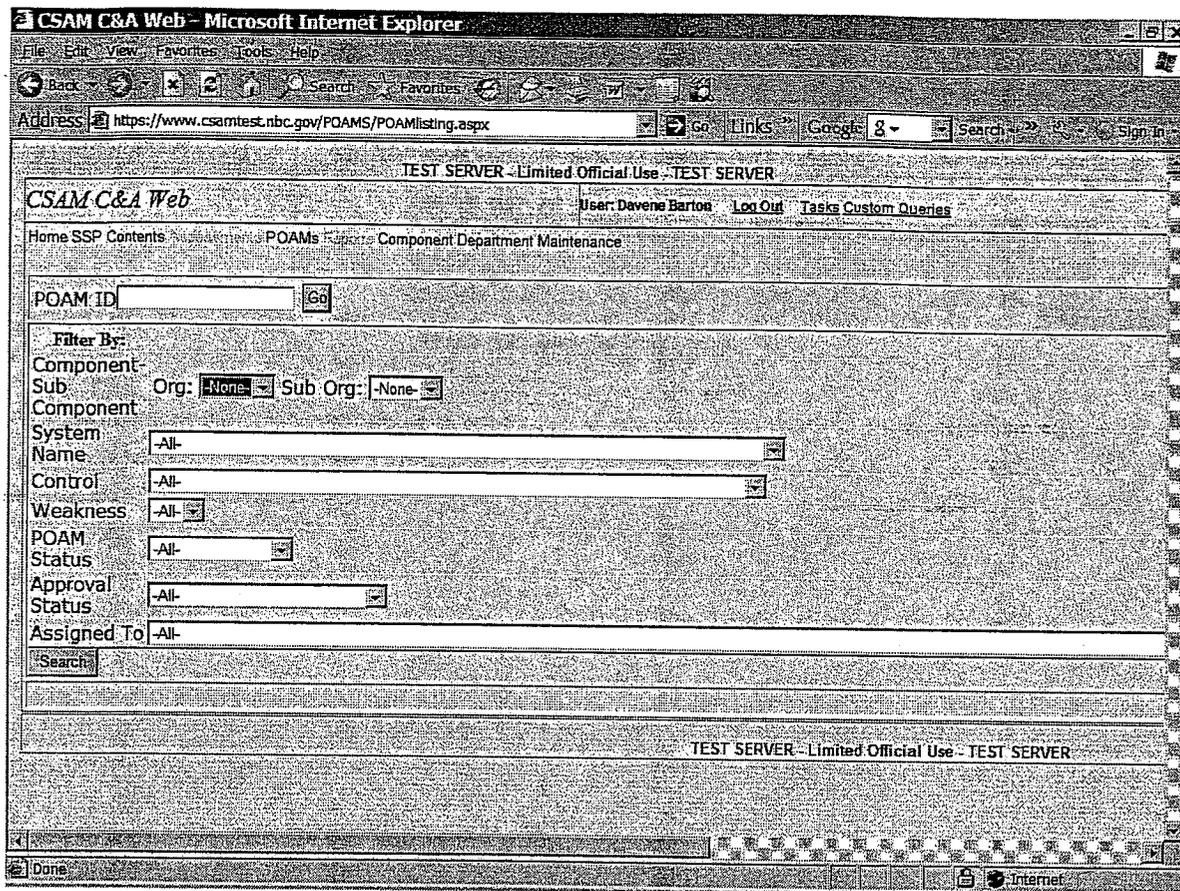
RTM Audit Reminders
 The following list shows SSPs that may require an adjustment to the current RTM Selection Factors:

SSP	Factor	Recommended Value	Actual Value
10 Gas	SecurityCategory	Low	Moderate
10 Gas	Financial	No	Yes
29 Gas	Financial	No	Yes
30 Gss	Financial	No	Yes
30 Gss	SecurityCategory	No Data	Moderate
35 MA	Financial	No	Yes
37 Gss	Financial	No	Yes
37 Gss	SecurityCategory	No Data	Moderate
61 MA	SecurityCategory	Moderate	Low
A Conversion Test	SecurityCategory	No Data	Low
Abandoned Mine Land Inventory System	SecurityCategory	No Data	Low
Accessibility Data Management System	SecurityCategory	Moderate	High
Accessibility Data Management System	Financial	No	Yes
AOCSS	Financial	No	Yes
BLM Enclave GSS	Financial	No	Yes
BLM Training Program	Financial	No	Yes
Enterprise Web	SecurityCategory	High	Low
Federal Aid Information Management System	Financial	No	Yes
MMS Network (exclude the WAN backbone)	Financial	No	Yes
Trust Funds Accounting System	Financial	No	Yes

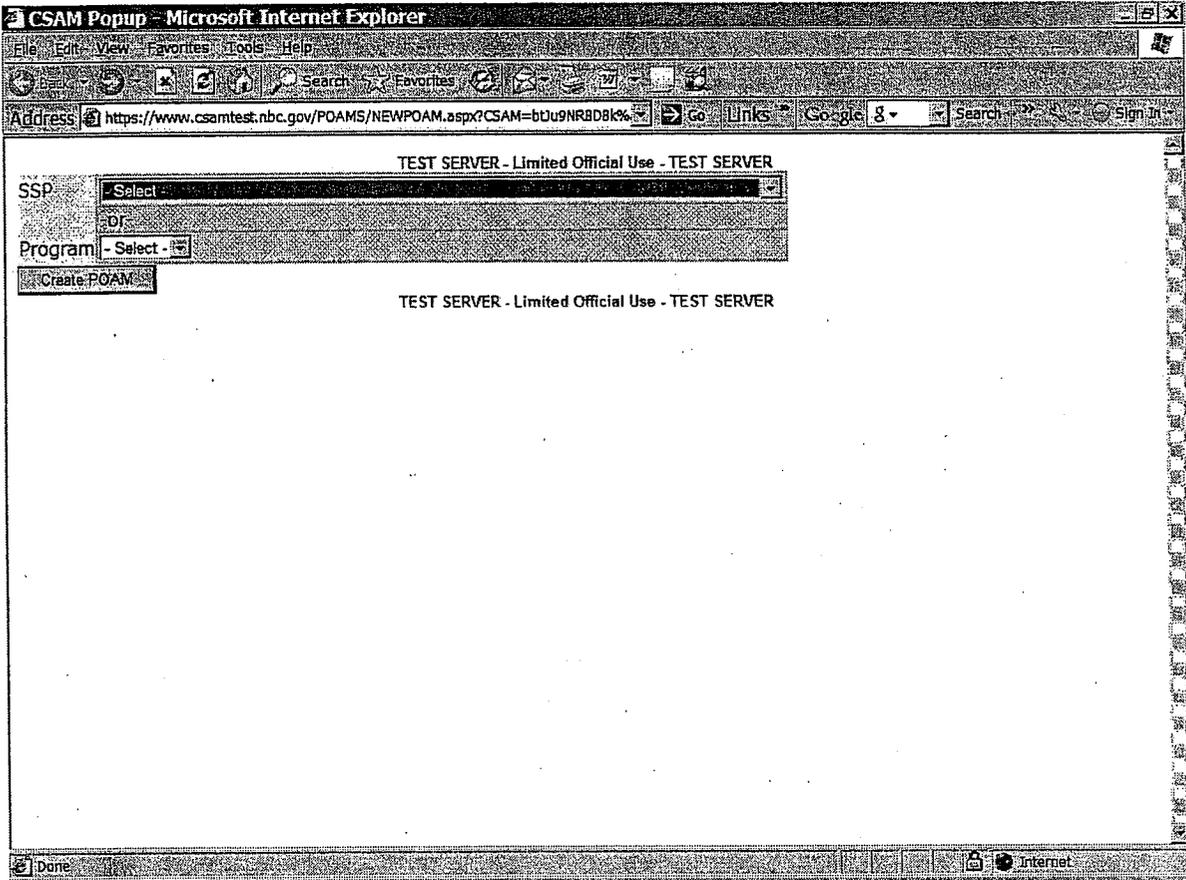
SSP Status Reminders

Done Internet

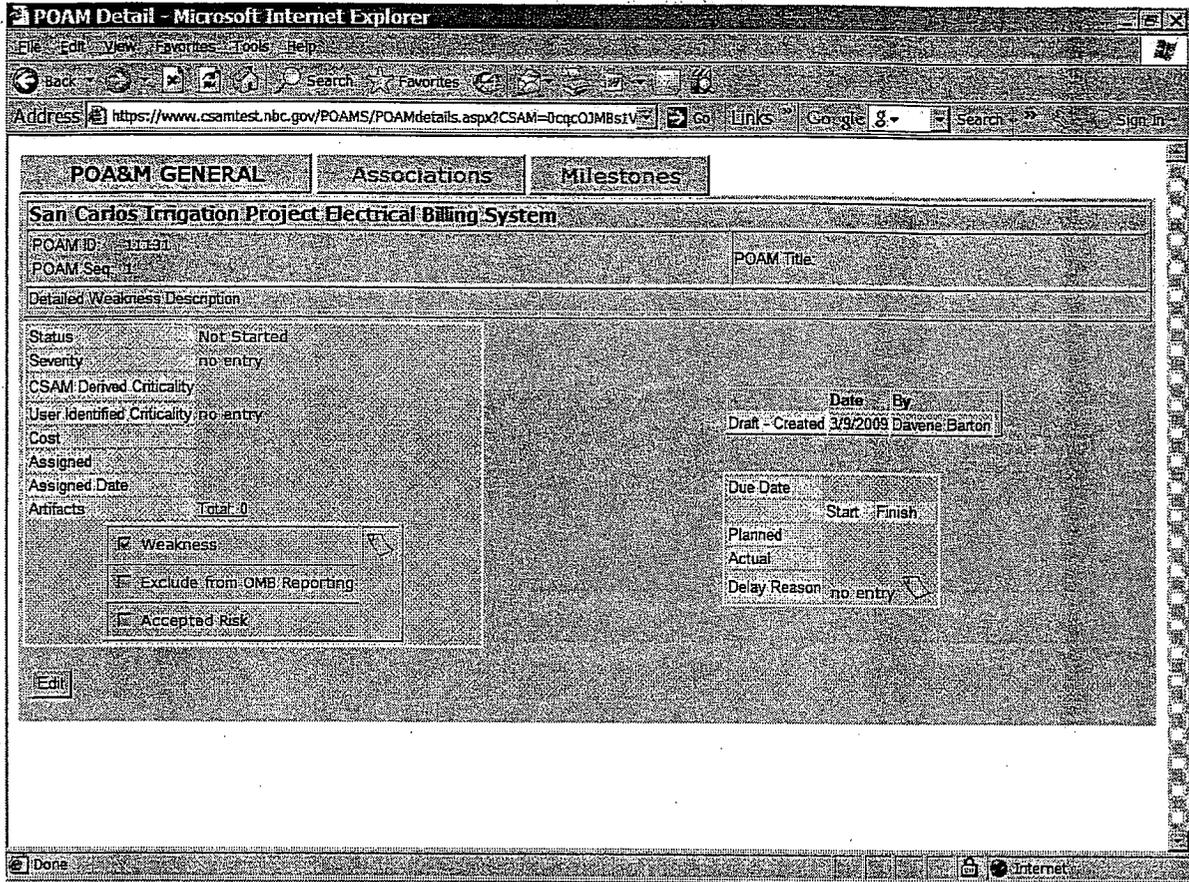
4. Select your bureau/office (Org) name, select System Name and then click the Add POA&M button located on the far right side of the screen.



5. Select the **Program** or **SSP** (system) name from the pick list and then select **Create POA&M**. (Note: Users will only have access to the systems/program specific to their bureau or office).



6. Select Edit.



The **POA&M ID** is a CSAM generated unique number for each POA&M. This number is unique amongst all system, site and program POA&Ms.

The **POA&M Seq.** is a CSAM generated unique number for each POA&M. This number is unique only within the system, site or program it belongs to. This number is sequentially assigned.

POA&M Detail - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address: <https://www.csamtest.nbc.gov/POAMS/POAMdetails.aspx?CSAM=0cqcOJMBs1V>

POA&M GENERAL | Associations | Milestones

San Carlos Irrigation Project Electrical Billing System

POAM ID: 11131 POAM Title: _____
 POAM Seq: _____

Detailed Weakness Description Full Screen Edit

Status: Not Started
 Severity: Other Weakness
 CSAM: _____
 Derived Criticality: _____
 User Identified: Very Low
 Cost: _____
 Assigned: -Select POC-
 Assigned Date: _____
 Artifacts Total: 0

Date By: Draft - Created 3/9/2009 Davenie Barton

Due Date: TBD
 Start: Planned: TBD, Actual: TBD
 Finish: TBD
 Delay: -No Selection-

7. Enter POA&M Title - a brief description of the weakness.
8. Enter Severity by clicking the drop-down menu and choosing the applicable option. The options are as follows:
 - a. **Other Weakness:** The PAO&M is not related to a specific control and was determined in a fashion other than the other options available for selection.
 - b. **Control Deficiency:** The POA&M is related to a control that is not implemented for a given system/program.
 - c. **Significant Deficiency:** The POA&M is not related to a specific control that is not implemented, rather the POA&M is related to another significant finding.
 - d. **Reportable Condition (Deprecated):** Deprecated means that this option should no longer be used by or selected by the user.
 - e. **Material Weakness:** The POA&M is not related directly to a control that is not implemented, rather the POA&M was found as a material weakness by an external examination (audit or some other means).

9. Enter Detailed Weakness Description. Enter the detailed weakness description in the text box.

POA&M Detail - Microsoft Internet Explorer

Address: <https://www.csamtest.nbc.gov/POAMS/POAMdetails.aspx?CSAM=0cqc0JMBs1V>

POA&M GENERAL | Associations | Milestones

San Carlos Irrigation Project Electrical Billing System

POAM ID: 11131 | POAM Title:

POAM Seq:

Detailed Weakness Description Full Screen Edit

Status: Not Started

Severity: Other Weakness

CSAM

Derived Criticality

User

Identified Criticality: Very Low

Cost:

Assigned: -Select POC-

Assigned Date

Artifacts: Total: 0

Due Date	Start	Planned	Actual	Delay
TBD		TBD	TBD	-No Selection-

10. **CSAM Derived Criticality.** CSAM automatically ranks the criticality of a POA&M when the vulnerability is associated at the Control or Expected Results level and is unaware of the operating environment of the system (i.e., is not aware of any mitigating/compensating controls that would justify any lower risk rating – e.g., a vulnerable port/service might have an initial risk rating of high but when taking into consideration an external firewall that prevents any other system from accessing the vulnerable port/service the user identified risk level might be adjusted to medium or low).

The **CSAM Derived Criticality** value is dynamically updated as the associated control implementation status changes. In the event the vulnerability is not associated at the control or expected result level, the user identified criticality level must be populated. An example of this may be Program related vulnerabilities.

11. Select the **User Identified Criticality** of the POA&M from the pick list. Using data from a user defined risk assessment process, enter appropriate the criticality level. (Note: The User Identified Criticality level is the “official criticality level” to the extent that it is selected/identified as instructed by this POA&M Process Standard. If it is not adjusted

by the user then the “official-criticality level” would default to the “CSAM-Derived Criticality”.

12. Enter the **Cost** information. POA&M cost can be captured and associated with the POA&M, providing visibility on several other CSAM screens. This capability enables IT Security Specialists and management to make credible, risk-based decisions with regard to the operation and use of information systems.

POAM Detail - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://www.csamtest.nrc.gov/POAMS/POAMdetails.aspx?CSAM=0cqc0JM8s1V> Go Links Google Search Sign In

POA&M GENERAL Associations Milestones

San Carlos Irrigation Project Electrical Billing System

POAM ID: 11131 POAM Title:

POAM Sec:

Detailed Weakness Description Full Screen Edit

Status: Not Started

Severity: Other Weakness

CSAM Derived Criticality: Very Low

User Identified:

Cost:

Assigned: -Select POC-

Assigned Date:

Artifacts Total:

Date By: Draft - Created 3/9/2009 Davene Barton

Due Date: TBD Auto-Schedule: Select a Schedule

Planned Start: TBD Planned Finish: TBD

Actual Start: TBD Actual Finish: TBD

Delay: -No Selection-

Done

13. Enter **Assigned POC**. This assignment is made from a drop down table of POCs for which CSAM contains contact information online.
14. Enter the **Due Date** also known as the Schedule Completion Date (SCD). This date is the key date that will be locked-down as the baseline, once the POA&M is approved. While in Draft POA&M status, this value can be changed. The user has the option to enter dates directly into individual fields or use the auto-scheduler to set the **Due Date**, **Planned Start** and **Planned Finish** dates, however, the user must enter the **Actual Start** and **Actual Finish** dates manually.
15. Select **Yes** or **No** from the **Created as a Result of an OIG Evaluation** pick list, enter the **Source of Weakness**. When entering the source of weakness information bureaus/offices must include the title of the report, the report

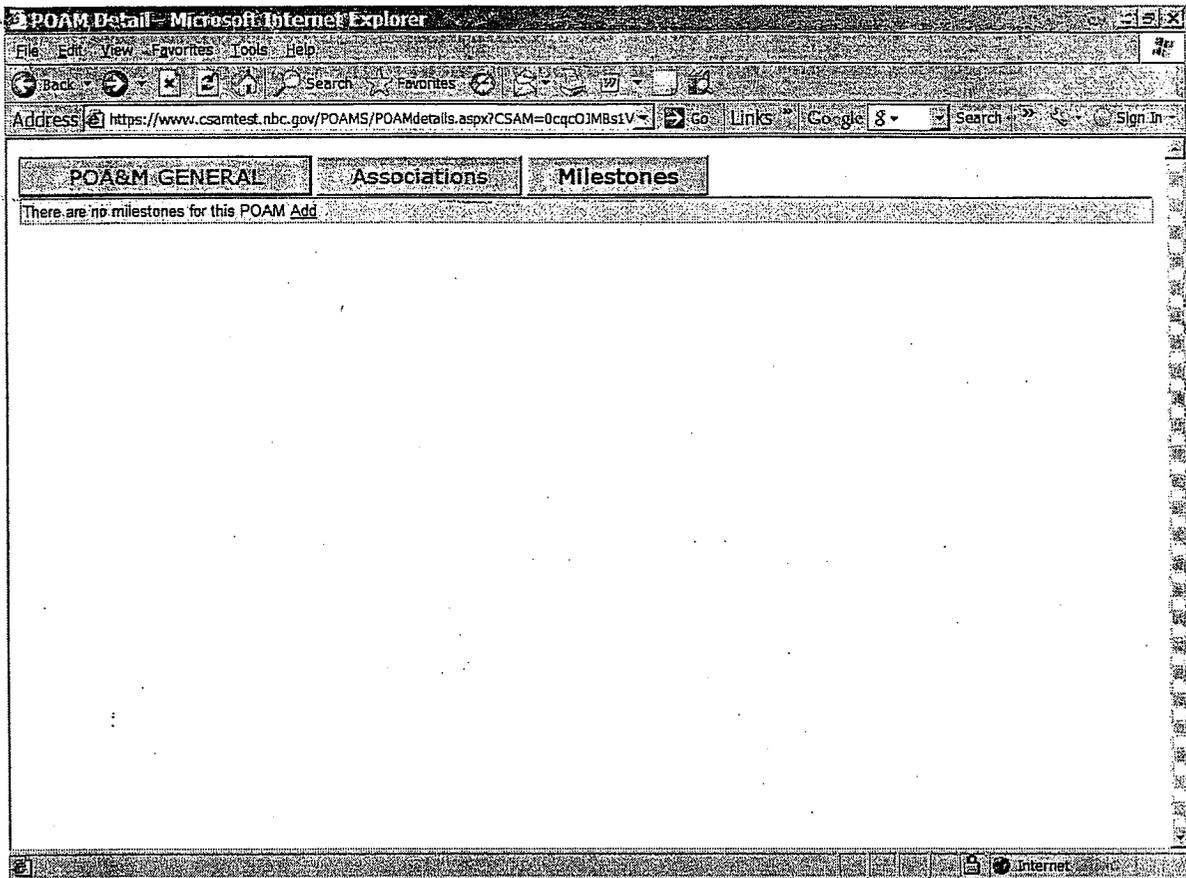
number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness.
Click Save

POAM ID: 15660
POAM Seq: 47 Print POAM
POAM Title: _____
Detailed Weakness Description: Full Screen Edit

Status: Not Started
Severity: Other Weakness
CSAM Derived Criticality: _____
User Identified Criticality: Low
Cost: _____
Assigned: Select POC
Assigned Date: _____
Artifacts: Total: 1
 Weakness
 Exclude from OMB Reporting
 Accepted Risk
0 Weakness comments. Click to Add.

Created as a Result of an OIG Evaluation: Yes
Source of Weakness: _____
Save Delete Cancel

16. Select the Milestones tab and then select Add.
17. Enter milestones in the order they should be executed.



Note: The key milestones associated with each corrective action should be identified on each POA&M. Each weakness must have one or more associated milestones. Milestones should define the major steps that will be performed to complete the corrective action. If there is more than one milestone, enter the milestone in the order they should be executed. For example, one set of milestones for a weakness such as, "Identification and authentication are not adequate for the level of security controls required for this system" might be:

- 1) Evaluate methods for strengthening identification and authentication.
- 2) Recommend solution and obtain approval.
- 3) Develop procedures to standardize accepted identification and authentication process.
- 4) Design identification and authentication solution.
- 5) Build identification and authentication solution.
- 6) Test identification and authentication solution.
- 7) Deploy identification and authentication solution and implement supporting process.

Milestones might also include more specific aspects related to the technical solution (e.g. implement two-factor authentication), and management and operational controls related to the steps for implementing supporting business practices and procedures where additional security control requirements are known or anticipated.

The description of each milestone must be detailed enough so that an independent reviewer will understand the planned corrective action and determine whether the corrective action is adequate and appropriate and will result in the weakness being corrected or its associated risk mitigated to a level acceptable to the AO. The last milestone entry must clearly identify the action taken to mitigate the weakness. Sensitive information can be included as needed for the description since the entire POA&M is a sensitive but unclassified document.

18. Select **Update** to save the entry.

The screenshot shows a web browser window titled "POAM Detail - Microsoft Internet Explorer". The address bar shows the URL: <https://www.csamtest.nbc.gov/POAMS/POAMdetails.aspx?CSAM=0cqc0JMBs1V>. The page content is organized into tabs: "POA&M GENERAL", "Associations", and "Milestones". The "Milestones" tab is selected, displaying a table with the following columns: "Add", "Milestone", "Due", "Planned Start", "Planned Finish", "Actual Start", and "Actual Finish". Below the table, there is a form for editing a milestone. The "Due" field is set to "3/9/2009". There is an "Assigned To:" field with a dropdown menu. At the bottom of the form, there are buttons for "Update", "Cancel", "Edit", and "Delete". The status bar at the bottom of the browser shows "Done" and "Internet".

19. Select the POA&M General tab and then select Edit.

POA&M GENERAL Associations Milestones

OS Program

POAM ID: 14235 POAM Title: OTG Evaluation(Recommendation#) Brief Description
 POAM Seq: 72 Detailed Weakness Description Full Screen Edit

Description

Status: Not Started
 Severity: Other Weakness
 CSAM
 Derived
 Criticality
 User
 Identified: Low
 Criticality
 Cost: 10

Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438

Assigned Date

Artifacts Total: 0

Date: By
 Draft - Created 2/15/2009 Davene Barton

-Status Change Request Options- Submit

Due Date: 3/17/2009 Auto Schedule: 20 Days
 Start: Finish:
 Planned: 2/15/2009 3/17/2009
 Actual: TBD TBD

20. Select **Draft - Approval Requested** from the Status Change Request Options pick list and then click **Submit**.

POA&M GENERAL **Associations** **Milestones**

OS Program

POAM ID: 14235 POAM Title: _____
 POAM Seq: 172 OIG Evaluation(Recommendation=) Brief Description: _____

Detailed Weakness Description/Full Screen Edit

Description

Status: Not Started
 Severity: Other Weakness
 CSAM
 Derived: _____
 Criticality: _____
 User: _____
 Identified: Low
 Criticality: _____
 Cost: 10
 Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438
 Assigned Date: _____
 Artifacts Total: 0

Draft - Approval Requested

Date: By: _____
 Draft - Created 2/15/2009 Davene Barton

-Status Change Request Options- Submit

-Status Change Request Options-
Draft - Approval Requested

Due Date	3/17/2009	Auto Schedule	30 Days
Planned	2/15/2009	Finish	3/17/2009
Actual	TBD		TBD

21. To approve entry of the POA&M, select **Edit, POA&M Approved** from the **Status Change Request Options**, provide comments and then click **Submit**.

POA&M GENERAL Associations Milestones

OS Program

POAM ID: 14235 POAM Title: OTG Evaluation(Recommendation#) Brief Description

POAM Seq: 72

Detailed Weakness Description Full Screen Edit

Description

Status: Not Started

Severity: Other Weakness

CSAM

Derived

Criticality

User Identified: Low

Criticality

Cost: 10

Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438

Assigned Date: 2/15/2009

Artifacts Total: 0

Date	By
Draft - Created 2/15/2009	Davene Barton
Draft - Approval Requested 2/15/2009	Davene Barton
Draft - Approval Requested 2/15/2009	Davene Barton

-Approval Options- Submit

-Approval Options-

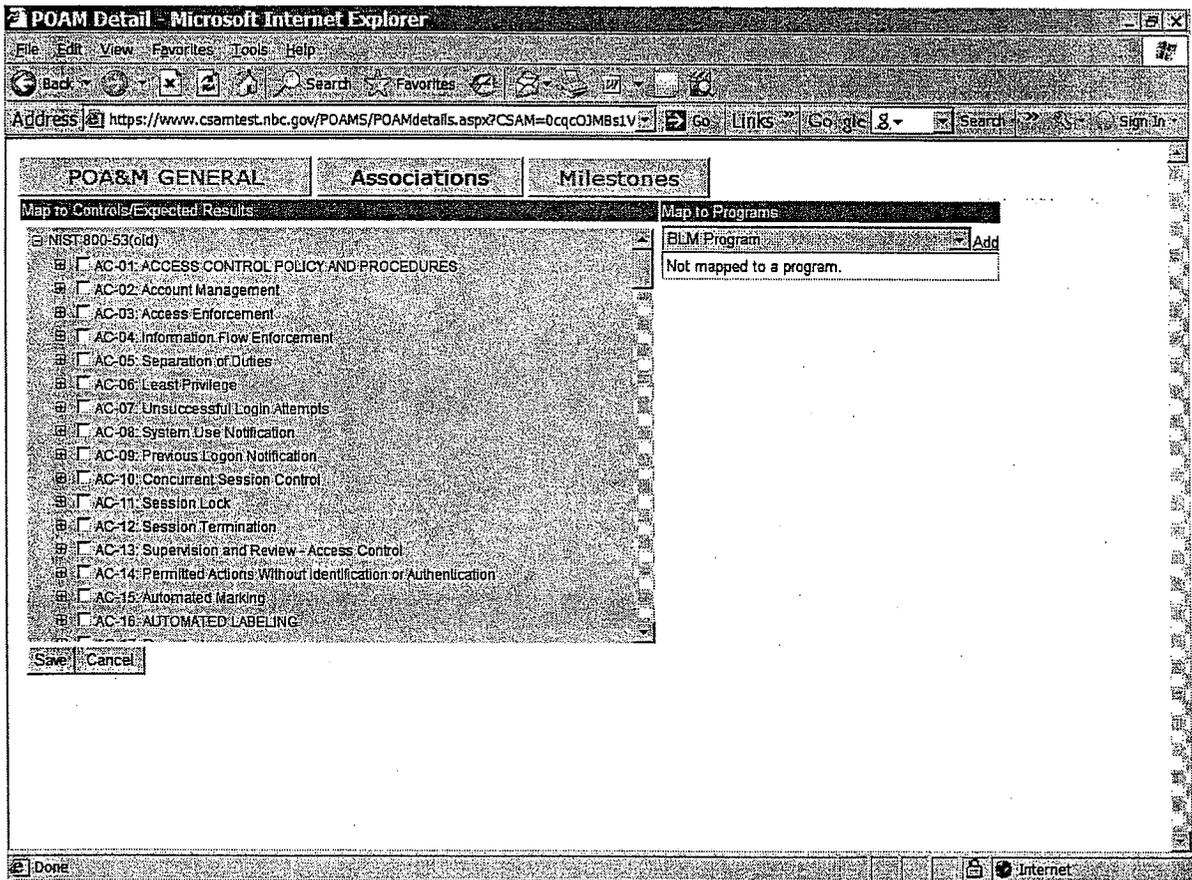
POAM Approved

POAM Approval Denied

Due Date: 3/17/2009 Auto Schedule

Select a Schedule

23. Select **Edit**.
24. Select applicable controls.
25. Select a Program to add (if applicable) and then select **Add**.
26. Select **Save**.
27. Select the **POA&M General Tab** and exit the application. This completes the POA&M creation work flow process.



28. To close a POA&M weakness, select the POA&Ms link.

CSAM C&A Web Home - Microsoft Internet Explorer

Address: https://www.csamtest.nbc.gov/CSAMCentral.aspx

TEST SERVER - Limited Official Use - TEST SERVER

CSAM C&A Web User: Davene Barton Log Out Tasks Custom Queries Help

Home SSP Contents POAMs Component Department Maintenance

RTM Audit Reminders
The following list shows SSPs that may require an adjustment to the current RTM Selection Factors.

SSP	Factor	Recommended Value	Actual Value
10 Gss	SecurityCategory	Low	Moderate
10 Gss	Financial	No	Yes
29 Gss	Financial	No	Yes
30 Gss	Financial	No	Yes
30 Gss	SecurityCategory	No Data	Moderate
35 MA	Financial	No	Yes
37 Gss	Financial	No	Yes
37 Gss	SecurityCategory	No Data	Moderate
61 MA	SecurityCategory	Moderate	Low
A Conversion Test	SecurityCategory	No Data	Low
Abandoned Mine Land Inventory System	SecurityCategory	No Data	Low
Accessibility Data Management System	SecurityCategory	Moderate	High
Accessibility Data Management System	Financial	No	Yes
AOCGSS	Financial	No	Yes
BLM Enclave GSS	Financial	No	Yes
BLM Training Program	Financial	No	Yes
Enterprise Web	SecurityCategory	High	Low
Federal Aid Information Management System	Financial	No	Yes
MMS Network (exclude the WAN backbone)	Financial	No	Yes
Trust Funds Accounting System	Financial	No	Yes

SSP Status Reminders

29. Select your bureau/office(Org) name, select System Name and then select Search:

The screenshot shows a web browser window titled "CSAM C&A Web - Microsoft Internet Explorer". The address bar contains the URL "https://www.csamtest.nbc.gov/POAMS/POAMlisting.aspx". The page header includes "TEST SERVER - Limited Official Use - TEST SERVER" and "CSAM C&A Web". Below the header, there are navigation links: "Home", "SSP", "Contents", "POAMs", and "Component Department Maintenance". The main content area features a search form with the following fields and options:

- POAM ID:
- Filter By:
- Component:
- Sub: Org: Sub Org:
- System Name:
- Control:
- Weakness:
- POAM Status:
- Approval Status:
- Assigned To:
-

The page footer includes "TEST SERVER - Limited Official Use - TEST SERVER" and a status bar showing "Done" and "Internet".

30. Enter the POA&M ID that you would like to close and select Go.

CSAM C&A Web - Microsoft Internet Explorer

Address: https://www.csam.nbc.gov/POAMS/POAMlisting.aspx

Limited Official Use

CSAM C&A Web User: Davene Barton Log Out Tasks Custom Queries

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

POAM ID: Go

Filter By:

Component Sub Org: OS Sub Org: None

Component System Name: OS Program

Control: All

Weakness: All

POAM Status: All

Approval Status: All

Assigned To: All

Search:

56 row(s) returned

POAM ID	POAM Seq	Component	Subcomponent	System Name	System Acronym	POAM Title	
10888	1	OS		OS Program		ISD-EV-MOA-0005-2007-OS-CSD-07-00008: OIG Recommendation #8- Enhance Plan of Actions & Milestone	05/0
				OS		ISD-EV-MOA-0005-2007-OS-CSD-05-00005: The DOI-CIO should	

Start Mail - Inbo... Online Ban... CSAM C&A... CSAM CR... CSAM POA... 9:20 AM

3.1. Select Edit

POAM Detail - Microsoft Internet Explorer

Address: <https://www.csam.nrc.gov/POAMS/POAMdetails.aspx?CSAM=QV3UJNAezhltU0g10SA%3d%3d>

POA&M GENERAL **Associations** **Milestones**

OS Program

POAM ID: 14235 POAM Title: OIG Evaluation (Recommendation #) - Brief Description
 POAM Seq: 72

Detailed Weakness Description
 Description:

Status: Planned/Pending
 Severity: Other Weakness
 CSAM Derived Criticality:
 User Identified Criticality: Low
 Cost: 10
 Assigned: Davene Barton
 Assigned Date: 2/15/2009
 Artifacts: Total: 0

Weakness
 Exclude from OMB Reporting
 Accepted Risk

Created as a Result of an OIG Evaluation: Yes
[Edit](#)

	Date	By
Draft - Created	2/15/2009	Davene Barton
Draft - Approval Requested	2/15/2009	Davene Barton
Draft - Approval Requested	2/15/2009	Davene Barton
POAM Approved	2/15/2009	Davene Barton

Due Date	Start	Finish
3/17/2009	2/15/2009	3/17/2009

Actual:
 Delay Reason: no entry

Taskbar: Start, Windows Explorer, Mail - Inbox, Final OIG Reco..., Document..., Component P..., POAM Detail..., 6:41 PM

32. Select POA&M Close Requested, from the Status Change Request Options, provide comments and then click Submit.

POA&M GENERAL Associations Milestones

DS Program

POAM ID: 14285 POAM Title: _____
 POAM Seq: 72 OIG Evaluation(Recommendation#): _____
 Brief Description: _____

Detailed Weakness Description: Full Screen Edit

Description: _____

Status: Planned/Pending
 Severity: Other Weakness
 CSAM: _____
 Derived: _____
 Criticality: _____
 User Identified: Low
 Criticality: _____
 Cost: 10

Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438
 Assigned Date: 2/15/2009
 Artifacts Total: 1

Date	By
Draft - Created	2/15/2009 Davene Barton
Draft - Approval Requested	2/15/2009 Davene Barton
Draft - Approval Requested	2/15/2009 Davene Barton
POAM Approved	2/15/2009 Davene Barton

Status Change Request Options

- Status Change Request Options-
- Status Change Request Options-
- POAM Cancellation Requested
- POAM Close Requested**

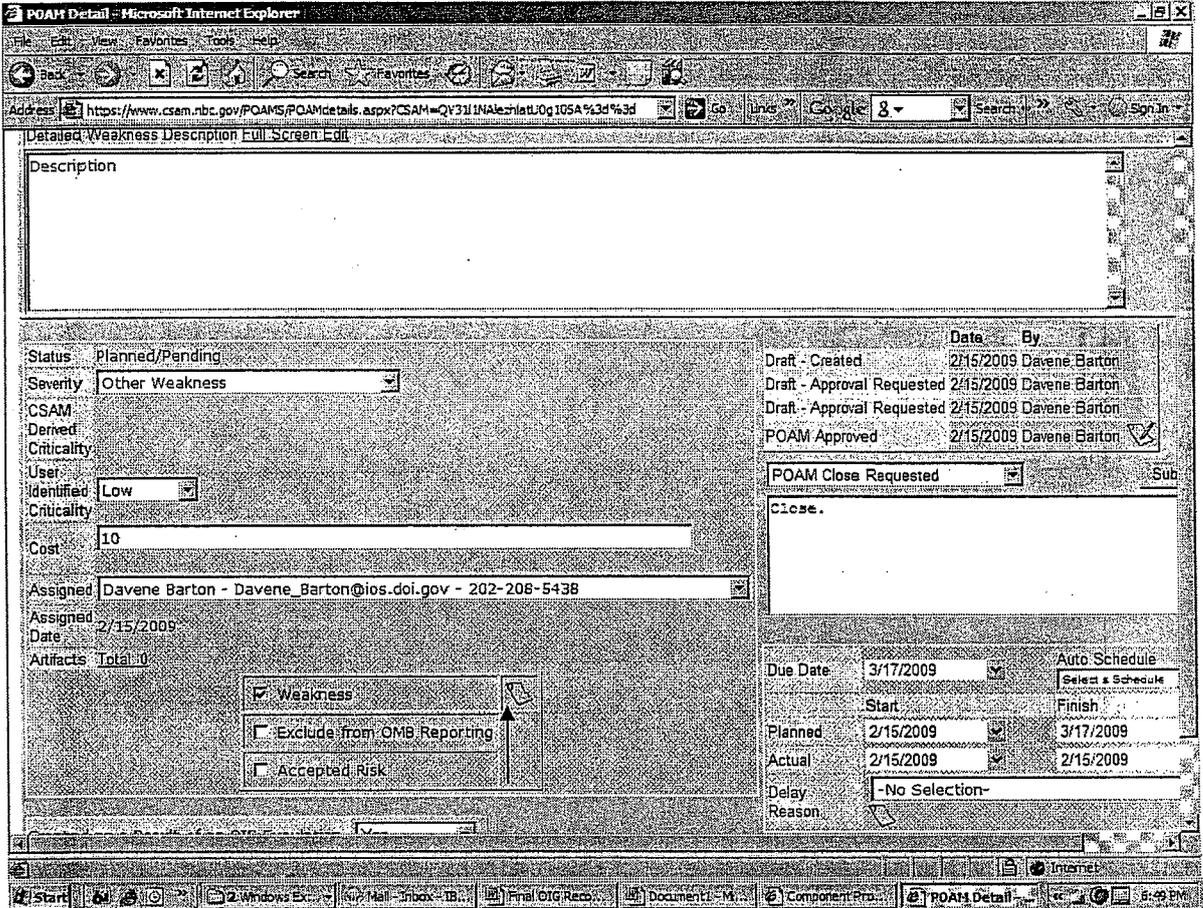
Submit

Done

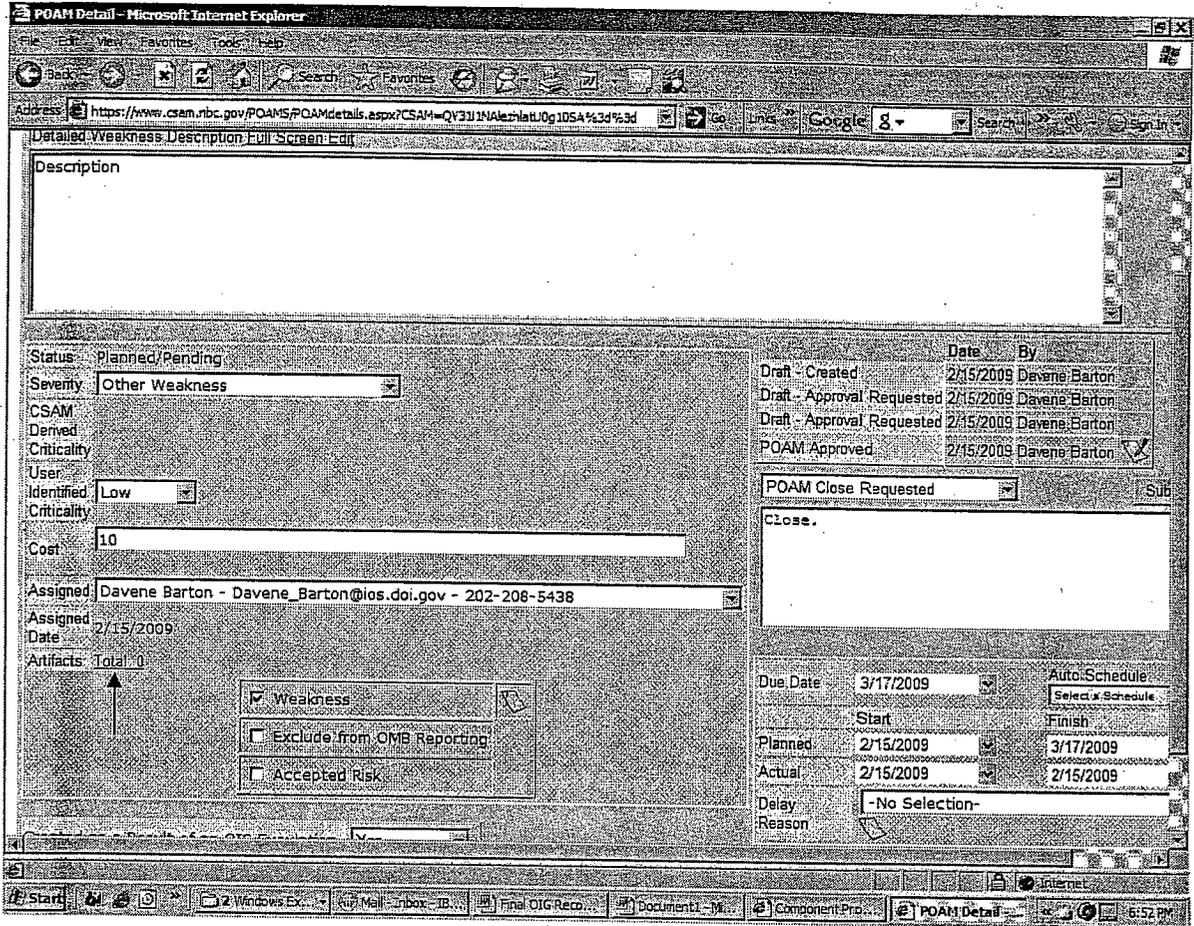
Start 2 Windows Ex... Mail (Box) - B... Final OIG Rec... Documents - M... Component Pro... POAM Detail... 6:42 PM

Note: After a POA&M weakness has been closed there are limited capabilities to modify them. Please ensure that newly created POA&Ms are in compliance with this standard. All POA&M weaknesses that are closed but are found to be non-compliant must be corrected or re-created with a reference to the original POA&M ID number in the POA&M Title field. The re-created (new) POA&M must reference the original POA&M ID number in the "POA&M Title" field. Additionally, the original (old) POA&M must reference the re-created POA&M ID number in the "POA&M Title" field.

33. Select the paper icon located next to Weakness, Select Add Comment, enter the corrective action(s) in the comment field and select Update.



34. Select the **Total** icon, to the left of **Artifacts**, upload artifacts such as WCVFs, screenshots, memorandum signature pages and other relevant evidentiary artifacts that clearly demonstrate successful resolution of the weakness.



35. To upload CIO and AO Transmittal Memos, return to the home page, select **Component** and then **Shared Artifacts**.

The screenshot displays the CSAM C&A Web application interface. At the top, the browser title is "CSAM C&A Web Home - Microsoft Internet Explorer" and the address bar shows "https://www.csam.nbc.gov/CSAMCentral.aspx". The page content is organized into several sections:

- Navigation:** A menu bar includes "Home", "SSP", "Contents", "Assessments", "POAMs", "Reports", "Component", "Department", "Maintenance", and "My Account". The "Component" menu is expanded, showing options like "Programs", "Dashboards", "FISMA Reports", "Enter Monthly Training Data", "POC Maintenance", "POAM Report (Component SSPs Only)", "Enable/Disable Email by Component", and "Shared Artifacts".
- Accreditations Table:** A table titled "Accreditations Expiring in 30 days or Less" with columns for "SSP", "Status", and "ATO".

SSP	Status	ATO
BLM - Land and Resources Project Office Major Application	ATO	10/18/2009
BLM - Wild Horse and Burro Information System	ATO	10/18/2009
BOR - GPSCADAS - Wyoming Area Office (WYAD)SCADA	ATO	9/25/2009
NBC - Momentum	ATO	9/27/2009
NBC - Oracle Federal Financials	ATO	9/27/2009
NBC - Drug Testing System	ATO	9/30/2009
OS - SID Alaska Local Area Network	ATO	9/31/2009
OS - Complaints	ATO	9/30/2009
OS - Recreation Information Database	ATO	10/24/2009
- POAM Reminders:** A section titled "POAM Reminders" with a search filter set to "Late" and a "Select Org" dropdown menu.
- Shared Artifacts:** A section titled "Shared Artifacts" with a search filter set to "Late" and a "Select Org" dropdown menu.

36. Enter artifact Description, from the Component pick list select bureau or office name, from the Type pick list select Miscellaneous, select Upload to save the information, return to the POA&M module.

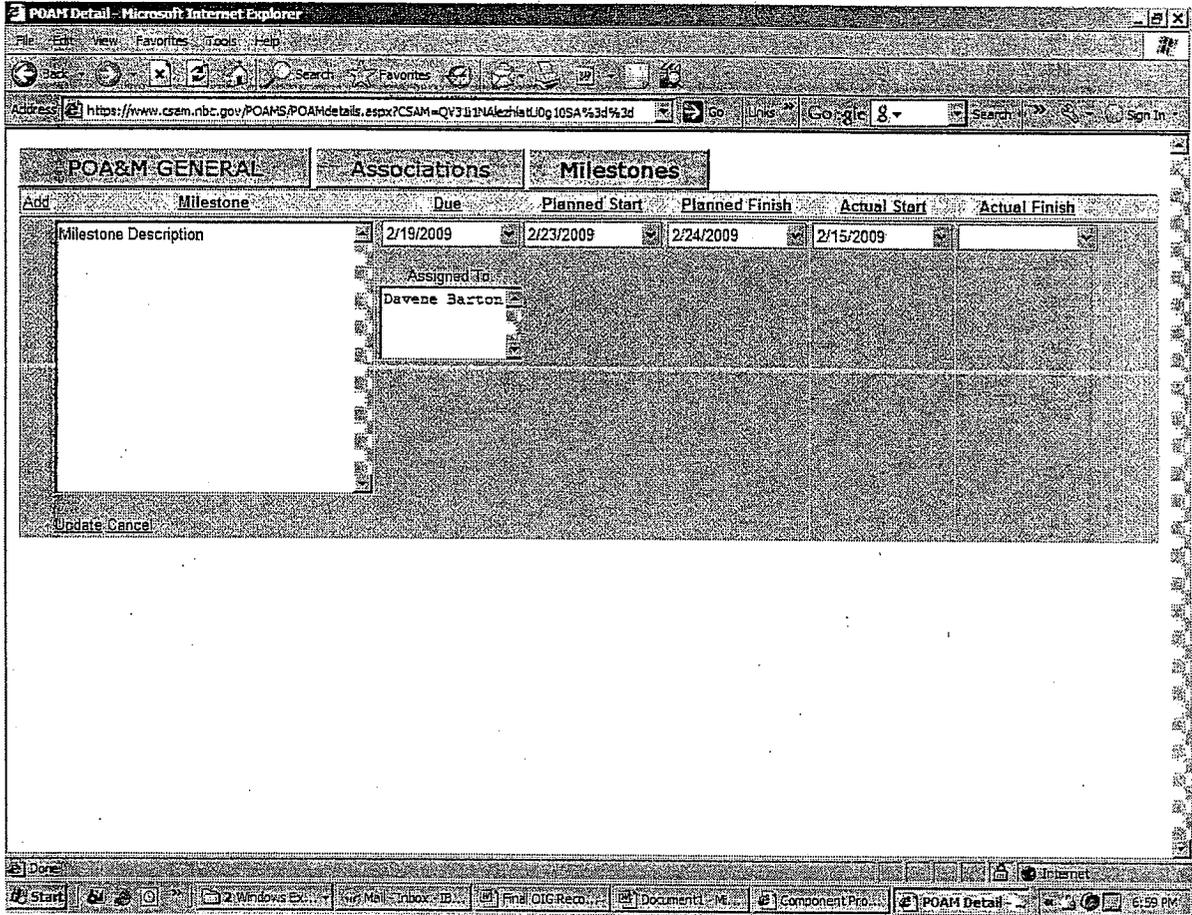
Microsoft Internet Explorer - Untitled Page

Address: https://www.csem.nbc.gov/Maintenance/SharedArts.aspx

Limited Official Use

Update	Description	Level	Component	Type	Updated	Update by	Action
Cancel		Department	Department Level Artifact	Global	Upload	New Row	dbarton
Delete							
Edi		Department			New Row	mybhe	
Edi		Department			New Row	rdowns	
Edi		Department			New Row	rdowns	
Edi	USGS FY09 Q4 DAA Memo	Component USGS		Miscellaneous	View	2:59:00 PM	hwinter
Edi	USGS FY08 Financial ICR Memo	Component USGS		Assessment	View	9/12/2009 3:07:00 PM	hwinter
Edi	USGS FY08 Q3 CIO/DAA Memo	Component USGS		Miscellaneous	View	9/12/2009 2:59:00 PM	hwinter
Edi	USGS FY08 Q4 CIO/DAA Memo	Component USGS		Miscellaneous	View	9/12/2009 2:54:00 PM	hwinter
Edi	USGS FY09 Q1 CIO/DAA Memo	Component USGS		Miscellaneous	View	9/12/2009 2:50:00 PM	hwinter
Edi	USGS FY09 Q2 CIO/DAA Memo	Component USGS		Miscellaneous	View	9/12/2009 2:47:00 PM	hwinter
Edi	BOR Certification and Accreditation Guide	Component BOR		SSP Level	View	8/21/2009 4:38:00 PM	bwamschke
Edi	DOI IT Security Policy Handbook v 3	Component BOR			View	8/21/2009 3:55:00 PM	bwamschke

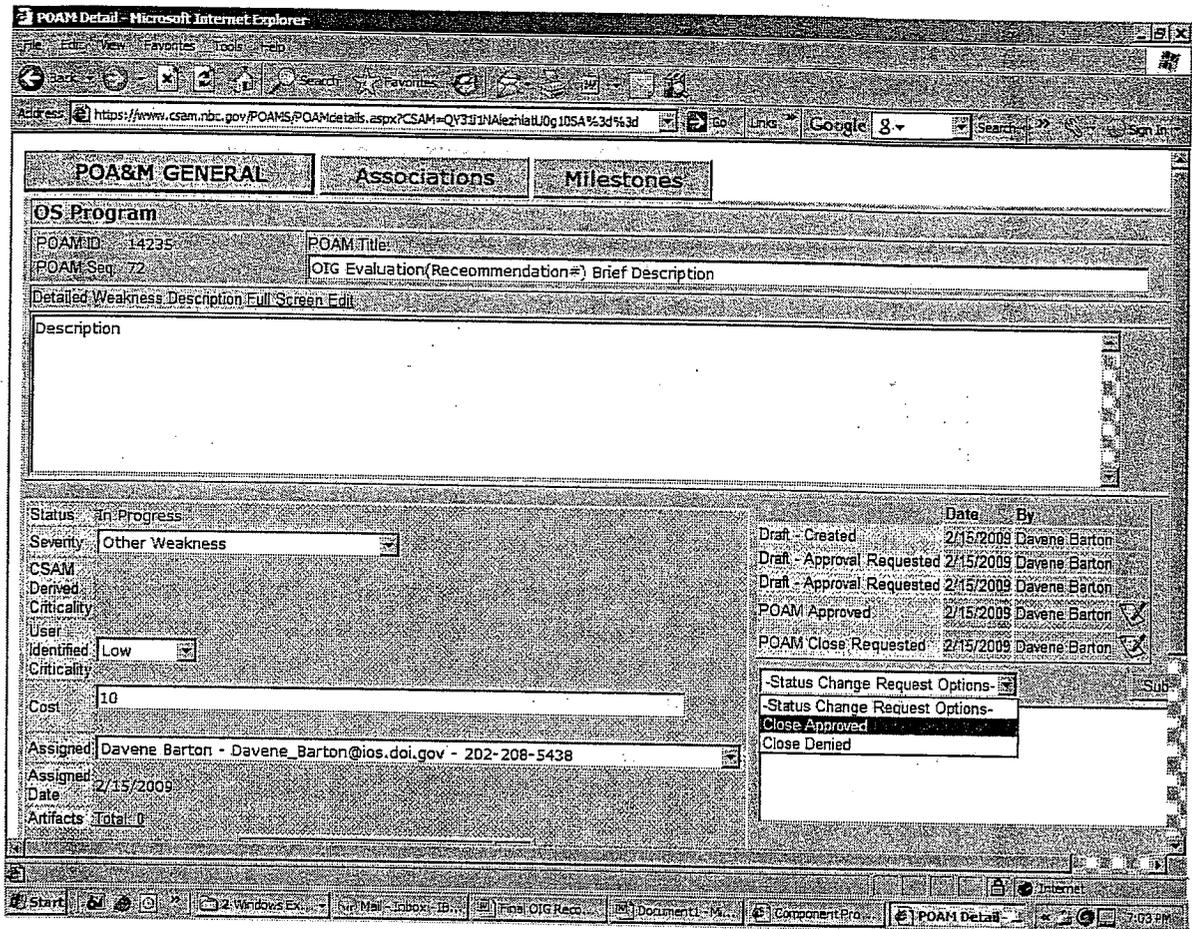
37. Select the **Milestones** tab and then click **Edit**.



38. Enter the milestone **Actual Finish** date.

39. Select **Update** to save the entry and then select the **POA&M General Tab**.

40. Select **Close Approved** from the Status Change Request Options, provide comments and then click **Submit**.



41. POA&M Approval Status options.

Draft Created: Each POA&M automatically starts in this state. A POA&M in this state can be deleted by any user who can edit the POA&M

Draft Approve Requested: When the key POA&M information has been entered and finalized, the user responsible for maintaining the POA&M selects this status to request approval. At least one milestone must have been entered before this event can be selected. Requires permission POAMEDIT.

POAM Approved: The user responsible for reviewing POAM Approval requests selects this status to indicate that the request has been approved. The user responsible for the POA&M can continue carrying out the actions and milestones associated with the POA&M. Once approved, the POA&M Title, Detailed Weakness Description, and Due Date fields are locked in read-only mode for regular users. Requires permission POAMAPPR or POAMAPSSP.

POAM Approval Denied: The user responsible for reviewing POAM Approval requests selects this status to indicate that the request has been denied. The user responsible for the POA&M can then make changes and resubmit the approval request. Requires permission POAMAPPR or POAMAPSSP.

POAM Auto Approved: The POA&M will automatically enter this state if it has not already been approved through the manual event process after 90 days from creation. The POA&M Title, Detailed Weakness Description, and Due Date fields are locked in read-only mode for regular users, with the exception that the Due Date field may be edited once if it was NULL when the POA&M was Auto-Approved.

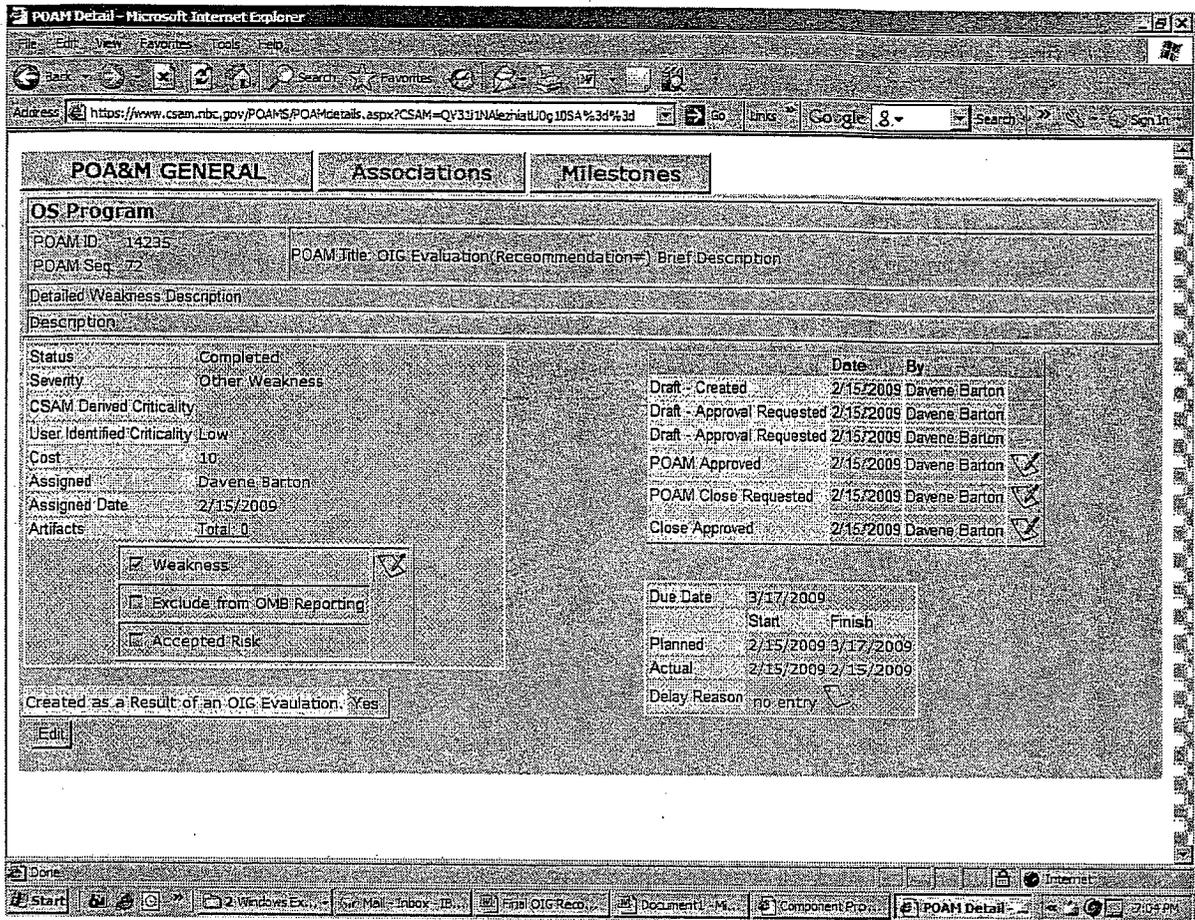
POAM Cancellation Requested: The user responsible for maintaining the POA&M can request cancellation if the POA&M has been approved and is still open. Typically this is done if the POA&M is a duplicate or if the requirement is no longer valid. Requires permission POAMCANCEL.

POAM Close Requested: The user responsible for maintaining the POA&M can request close if the POA&M has been approved and is still open. Typically this is done when after the POA&M actions and milestones have been carried out to completion. The POA&M Actual Start and Actual Finish dates must be populated before this event can be selected. Requires permission POAMCLOSE.

Cancel Approved: The user responsible for reviewing POAM Cancellation requests selects this status to indicate that the request has been approved. The POA&M status changes to Cancelled and no further actions are required on the POA&M. Requires permission POAMAPCANCEL.

Cancel Denied: The user responsible for reviewing POAM Cancellation requests selects this status to indicate that the request has been denied. The user responsible for the POA&M can then make changes and resubmit the cancellation request with a new justification, or work the actions and milestones to closure. Requires permission POAMAPCANCEL.

42. Enter the Actual Finish date and click Save to close the POA&M. The status will change from In Progress, Delayed or Ongoing to Completed.



The POA&M Status options are as follows:

Open/Closed: "Open" and "Closed" are not statuses that appear in the Status text field directly, but they are query options ("All Open" and "All Closed"). "All Open" is any POA&M that does not have status Cancelled or Completed. "All Closed" is any POA&M that has status Cancelled or Completed.

Not Started: A POA&M that has no actual start date and is Not Approved.

Planned/Pending: A POA&M that has a scheduled completion date, a planned start, and a planned finish date.

In Progress: A POA&M that has a scheduled completion date, a planned start, a planned finish date, an actual start date, and the POA&M is approved.

Delayed: When a user edits the POA&M, as well as when the nightly procedure executes, the status will be set to "Delayed" status if the POA&M is Approved and past its Due date, but does not currently have a status of "Delayed".

Denied: This is no longer a valid POA&M status. Previously, when the POA&M work flow status was one of the "denied" steps, the POA&M status would also read as "Denied." This was changed to no longer occur in CSAM v2.1. Some POA&Ms may still be in this state at this time if those POA&Ms have not been updated and changed state since the CSAM v2.1 deployment.

Cancelled: The POA&M work flow was moved to Cancel Approved, the POA&M status changes to Cancelled, no further actions are required on the POA&M.

Completed: The POA&M work flow was moved to Close Approved, the POA&M status changes to Closed, no further actions are required on the POA&M.

5 Conclusion

The benefits of the POA&M are significant and far-reaching, internally and externally to DOI. For each system, the POA&M serves as a comprehensive reference to be used in ongoing efforts to address programmatic and system-specific vulnerabilities. The POA&M is an essential management tool for the oversight and mitigation of security weaknesses. To function as an effective tool, POA&Ms must be continually and diligently updated. The operating environment, levels of acceptable risk, and the availability of resources are a small sampling of the many changes that occur on a frequent basis. An effective and successful POA&M document captures each one of these changes in a concise and complete fashion.

Appendix A: References

- Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, V2.0, June 2004.
- National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.⁵
- National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, October 2001.
- National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.
- National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.
- Office of Management and Budget Circular A-11, *Preparation, Submission and Execution of the Budget*, (Revised July 25, 2003).
- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, November 28, 2000.
- Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.
- Office of Management and Budget Memorandum M-02-09, *Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plan of Actions and Milestones*, July 2, 2002.
- Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 6, 2003.
- Office of Management and Budget Memorandum M-04-19, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*.
- Office of Management and Budget Memorandum M-05-15 *FY 2005 Instructions for Preparing the Federal Information Security Management Act Report and Privacy Management Report*.
- Public Law 107-347 [H.R. 2458], *The E-Government Act of 2002*, Title III, the *Federal Information Security Management Act of 2002* (FISMA), December 17, 2002.

⁵ This guidance is in process of revision and will map to NIST SP 800-53 Security Control Categories and provide additional functionality beyond the annual self-assessment.

Appendix B: Acronyms

AO	Authorizing Official
AOSS	All Other Sensitive Systems
BES	Business Essential System
BCISO	Bureau Chief Information Security Officer
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CSAM	Cyber Security Assessment and Management
CSD	Cyber Security Division
CTO	Chief Technical Officer
DAO	Designated Authorizing Official
DOI	Department of the Interior
DOJ	Department of Justice
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FTE	Full Time Equivalent
FY	Fiscal Year
GAO	General Accountability Office
GSS	General Support System
ICR	Internal Control Review
IG	Inspector General
INFOSEC	Information Security
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
MA	Major Application
MCS	Mission Critical System
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
PUB	Publication
RA	Risk Assessment
SSP	System Security Plan
UPI	Unique Project Identifier
WAN	Wide Area Network
WCVF	Weakness Completion Verification Form

Appendix C: Glossary

Acceptable Risk - a concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls.

Adequate Security - security that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Authorizing Official - (formerly known as Designated Approving Authority) official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Authorizing Official Designated Representative - individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.

Availability - ensuring timely and reliable access to and use of information.

Confidentiality - (1) assurance that information is not disclosed to unauthorized persons, processes, or devices. (2) Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Data Integrity - the property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

General Support System (GSS) - an interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data-processing center including its operating system and utilities, a tactical radio network, or a shared information-processing service organization.

Independent Reviewer - is responsible for validating that the corrective action was effectively implemented and that the completion status of the system security weakness has been accurately reported.

Information - any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Owner - is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the

data/information is shared with other organizations. This can be the business owner or in some cases the system owner at DOI.

Information Security (INFOSEC) - protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Information Technology (IT) - any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is used by DOI whether it is used directly or it is used by a contractor under a contract with DOI which: (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Integrity - (1) the degree to which a system (or system component) prevents unauthorized access to, or modification of, computer programs or data. (2) Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

IT Security Costs - In determining information and IT security costs, Federal agencies must consider the following criteria to determine security costs for a specific IT investment:

1. The products, procedures, and personnel (Federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. (Do not include activities performed or funded by the agency Inspector General.) This includes the costs of:
 - Risk assessment
 - Security planning and policy
 - Certification and accreditation
 - Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
 - Authentication or cryptographic applications
 - Education, awareness, and training
 - System reviews/evaluations (including security control testing and evaluation)
 - Oversight or compliance inspections
 - Development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment
 - Contingency planning and testing
 - Physical and environmental controls for hardware and software

• Auditing and monitoring

- Computer security investigations and forensics
 - Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations.
2. Products, procedures, and personnel (Federal employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; systems administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.
 3. Many agencies operate networks, which provide some or all the necessary security controls for the associated applications. In such cases, the agency must nevertheless account for security costs for each of the application investments. To avoid 'double-counting' agencies should appropriately allocate the costs of the network for each of the applications for which security is provided.

In identifying security costs, some agencies find it helpful to ask the following simple question, "If there was no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" Investments that fail to report security costs will not be funded; therefore, if the agency encounters difficulties with the above criteria they must contact OMB prior to submission of the budget materials.

Lead Responder – is responsible for ensuring that project or systems teams have taken appropriate remediation actions or steps to address, partially address, and/or recommend risk acceptance associated with system security weakness.

Major Application (MA) - an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function.

Major Information System - a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. Large infrastructure investments (e.g., major purchases of personal computers or local area network improvements) should also be evaluated against these criteria. Your agency Capital Planning and Investment Control (CPIC) Process may also define a major system or project. All major systems or projects must be reported on exhibit 53. In addition, a major IT system is one reported on your "Capital Asset Plan and Business Case," Exhibit 300. For the financial management mission area, major is any system that costs more than \$500,000. Additionally, if the project or initiative directly supports the President's Management Agenda Items, then the

project meets the criteria of high executive visibility. Projects that are E-government in nature or use e-business technologies must be identified as major projects regardless of the costs. If you are unsure about what systems to consider as major, consult your agency budget officer or OMB representative. Systems not considered "major" are "small/other".

Management Controls - techniques and concerns, normally addressed by an organization's management, that focus on the management of security and risk of an IT system. More expressly, actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions.

Material Weakness - or significant weakness is used to identify control weaknesses that pose a significant risk or threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.

Operational Controls - procedures and operational methods focusing on mechanisms implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

Plan of Action and Milestone (POA&M) - (a corrective action plan) a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Policy - a document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

Production System - Any system that stores, processes, or transmits live data or operates in a production environment.

Program Official - a division director or equivalent that is responsible for a major program or functional area.

Program Review - a program review, in the context of the work required under the Government Information Security Reform Act, is a review of the security status of an operational program and is not a security program itself. Each program must be reviewed annually to ensure: 1) risk assessments occur; 2) policies and procedures are risk-based and cost-effective and comply with existing laws and OMB policy; 3) security awareness training for all employees; 4) management testing and evaluation of the effectiveness of information security policies and procedures; 5) a process for remedial action; and 6) procedures for detecting, reporting, and responding to security incidents.

Reportable Condition - A reportable condition exists when a security or management control weakness does not rise to level of a significant deficiency, yet is still important enough to be reported to internal management. A security weakness not deemed to be a significant deficiency by agency management, yet affecting the efficiency and effectiveness of agency operations, may be considered a reportable condition. However, due to lower risk, corrective action may be scheduled over a longer period of time. A reportable condition under FISMA is not reported as a material weakness under FMFIA.

Residual Risk - is that risk remaining after all mitigation efforts have been implemented and any other potential corrective action strategies have been exhausted or otherwise determined to be cost-prohibitive when compared to the potential risk impact to the affected information technology system and its associated information/data.

Risk - the net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur.

Risk Assessment - the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.

Risk Management - the total process of identifying, controlling, and remediating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Security - technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. Also referred to IT Security.

Security Controls - the management, operational, and technical controls (i.e., safeguards or countermeasures), prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.

Security Program - a program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information technology systems.

Sensitive Data - information whose loss, misuse, unauthorized access to, modification, or destruction, could adversely affect the national interest or the conduct of Federal programs, or privacy to which individuals are entitled, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy, etc. Sensitive data can relate to industry (e.g., proprietary, patented), copyrighted or business data, as well as data that is simply inappropriate for public release.

Sensitivity - the degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components.

Significant Deficiency - is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. A significant deficiency under FISMA is to be reported as a material weakness under the Federal Managers Financial Integrity Act (FMFIA).

System - a collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected. (Defined in NIST SP 800-16, Appendix C). A system can also be defined as the interconnected set of information resources under the same direct management control, which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Technical Controls - automated, technological security mechanisms the IT system executes. The controls can provide automated protection for unauthorized access or misuse and facilitate detection of security violations.

Technical Reviewer - is responsible for ensuring that project or system team have taken appropriate remediation actions or steps to address, partially address, and/or recommend risk acceptance associated with the system security weakness. The technical reviewer is also responsible for ensuring all appropriate Security Technical Implementation Guide (STIGs) have been updated as noted.

Vulnerability - a flaw or weakness in a system's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Appendix D: Weakness Completion Verification Form

Completing Corrective Actions

In order to implement a needed security control and 'complete' a weakness, five levels of effectiveness must be met as follows:

1. The control objective must be documented in a security policy (e.g., the policy can either be a common control where the policy has been promulgated at the Departmental or bureau level, a system-specific policy issued as a rules of behavior (ROB) to users, etc.);
2. The security control must be documented as procedures (e.g., documented procedures, practices, security configuration guides (STIGs), etc.);
3. Procedures have been implemented;
4. Procedures and security controls are tested and reviewed; and
5. Procedures and security controls are fully integrated into a comprehensive program.

Three examples of appropriate corrective actions follow.

- **Management Control** - If the identified weakness was a lack of management controls (e.g., policies or standards), an appropriate corrective action might be development of a relevant and appropriate IT security policy. Adequate evidence that the corrective action was completed would be demonstrating that a final version of the policy was approved, signed, and promulgated by the responsible senior management official and disseminated and effectively communicated to individuals within the organization that needed to be informed and/or trained about the policy.

It may also be necessary to implement or update related operational and/or technical security controls consistent with the policies or standards developed to fully correct the identified weakness. Even though a security audit, test, or assessment failed to specifically identify these additional follow-on steps, the System Owner and other individuals responsible for the security of a system must take appropriate steps to identify any such additional activities and document on the POA&M by creating new POA&M entries, or by adding additional milestones to the existing related weakness, and then continue to implement corrective actions until all aspects of the weakness are addressed.

- **Operational Control** - If the identified weakness was a lack of operational controls (e.g., procedures, practices, or Security Technical Implementation Guides (STIGs)), an appropriate corrective action might be implementation of operational practices and procedures that are consistent with established and relevant IT security policies and standards. Adequate evidence that the corrective action was completed would be demonstrating that a final version of documented procedures exists and those responsible offices and individuals have been identified and have begun to effectively implement those practices.

It may also be necessary to implement or update related technical security controls consistent with existing policies or standards to support and help ensure efficient and

effective operational procedures and practices. Although the operational control should be able to demonstrate that it is compliant with a related management control, existence of the management control (although required) is not sufficient evidence that an operational control exists. Adequate evidence would include documented procedures and practices and evidence that implementation has been at least initiated by responsible offices and individuals.

- **Technical Control** - If the identified weakness was a lack of technical controls (e.g., security patches, operating system, application, database, web-services security configurations consistent with applicable STIGs, encryption of sensitive data or passwords, ineffective identification, authentication, or access controls, insufficient audit logging of security events, etc.), an appropriate corrective action might be implementation of appropriate device security configurations that corrects or mitigate the weakness, in a manner that is consistent with established and relevant IT security policies, standards, procedures, and practices.

Evidence that the corrective action was completed would be documentation of change records and associated approvals and completion signatures or other audit trails, results from independent vulnerability scanning tests using similar tools and methods of initial discovery, results from independent manual review of security configurations following similar inspection criteria and methodology used in initial discovery, etc. Although the technical control should be able to demonstrate that it has been implemented in a manner that is compliant with a related management control, existence of the management control (although required) is not sufficient evidence that the technical control exists, has been implemented correctly, and has been tested for effectiveness.

Weakness Completion Verification Form

The Weakness Completion Verification Form is embedded in the following logo.



Final WCVF Template
17 Mar 10.doc

Appendix E: POA&M Certification Transmittal

This section contains the templates of the Certification Transmittals to be completed by the CIO and AO and submitted as part of the quarterly POA&M submission.

The CIO Certification Transmittal is embedded in the following logo.



CIO Transmittal
Memo Template.doc

The AO Certification Transmittal is embedded in the following logo.



AO Transmittal Memo
Template.doc

Appendix F: Office of Inspector General Recommendation Status Reporting Process

Introduction

The Office of Inspector General (OIG) Information Security Division (ISD) conducts regular evaluations of IT security related functions throughout Interior. As IT security weaknesses are discovered the OIG generates reports to relay their recommendations to the affected bureaus and offices as well as to the Department's Office of the Chief Information Officer (OCIO).

All bureaus and offices must ensure that all OIG recommendations have a corresponding Plan of Action and Milestone (POA&M) in the Cyber Security Assessment and Management (CSAM) application. Bureaus and offices are required to provide quarterly updates in CSAM with a detailed status of remediating actions with regard to all open OIG recommendations since fiscal year 2007. In lieu of the adhoc process established in 2008 where bureaus and offices submitted their quarterly reports via word documents, effective FY 2009 Quarter 1, the updates must be entered into CSAM. The OIG will review POA&Ms created as a result of their evaluation in CSAM to make sure weaknesses are incorporated. The findings will be reviewed no less than quarterly to evaluate the effectiveness of corrective actions.

Within the OCIO, the Cyber Security Division (CSD) POA&M and Audit Liaison service area has been charged with the responsibility of providing oversight of the remediation actions by bureaus and offices as well as Departmental offices.⁶ In performance of CSD's oversight function, the CSD shall act as the central point of contact for reviewing, providing feedback, and tracking status of bureau, office, and Departmental updates to the OIG.

Purpose

The purpose of this document is to define a process by which the OCIO CSD shall coordinate the reporting of detailed resolution status of OIG recommendations on a quarterly basis. This document describes the methodology by which the POA&M and Audit Liaison shall collaboratively:

- Ensure bureaus and offices are aware of the deadlines for status reporting;
- Periodically review bureau and office updates in CSAM;
- Provide feedback to the bureaus and offices regarding required data elements.

Bureau/Office Responsibilities

⁶ Departmental Manual, Part 18, Paragraph 18.5(A) 1 requires the Department's "Information Technology Security Staff" to perform oversight.

Bureaus and offices are responsible for responding to each of their respective OIG report recommendations by creating a POA&M in CSAM. POA&Ms created as a result of an OIG evaluation must remain open until the CSD has the opportunity to re-evaluate them and confirms they are resolved to their satisfaction.

If the weakness has been remediated, enter the corrective action description as a milestone, change the **Status Change Request Option** to **Closure Requested** and upload evidentiary artifact(s) that demonstrate successful resolution (See Section 5, **POA&M Management** for more information on how to create and manage POA&Ms). Once the CSD has re-evaluated the POA&M weakness and determined that the weakness has been resolved to their satisfaction, the Bureau Chief Information Security Officer (BCISO) will be notified via e-mail from the CSD.

FISMA §3544(a) 2 requires policies and procedures to cost effectively reduce risk and periodically test information security controls to ensure they are effectively implemented. The Inspector General Act (as amended) §2 requires the OIG to promote economy, efficiency, and effectiveness. The purpose of requiring all OIG information security findings to be recorded in CSAM as a POA&M and require these POA&Ms to remain open until the CSD affirms they are resolved is to establish a procedure for ensuring the OIG's recommendations are addressed.

Bureaus and offices must also upload evidentiary artifacts in all updates whether the recommendation remains open or is closed. The CSD and OIG verifies accomplished milestones and progress in remediating weaknesses and require supporting evidence to do so. In addition to the Weakness Completion Verification Form (WCVF), at least one artifact that supports closure of the recommendation must be uploaded for every OIG recommendation that bureaus and offices have referenced as closed. Artifacts can be e-mails, screen shots, procedure documents etc., as long as the artifact provides sufficient and relevant detail to enable the OIG to conduct testing and/or evaluation of the effectiveness of the corrective actions taken.

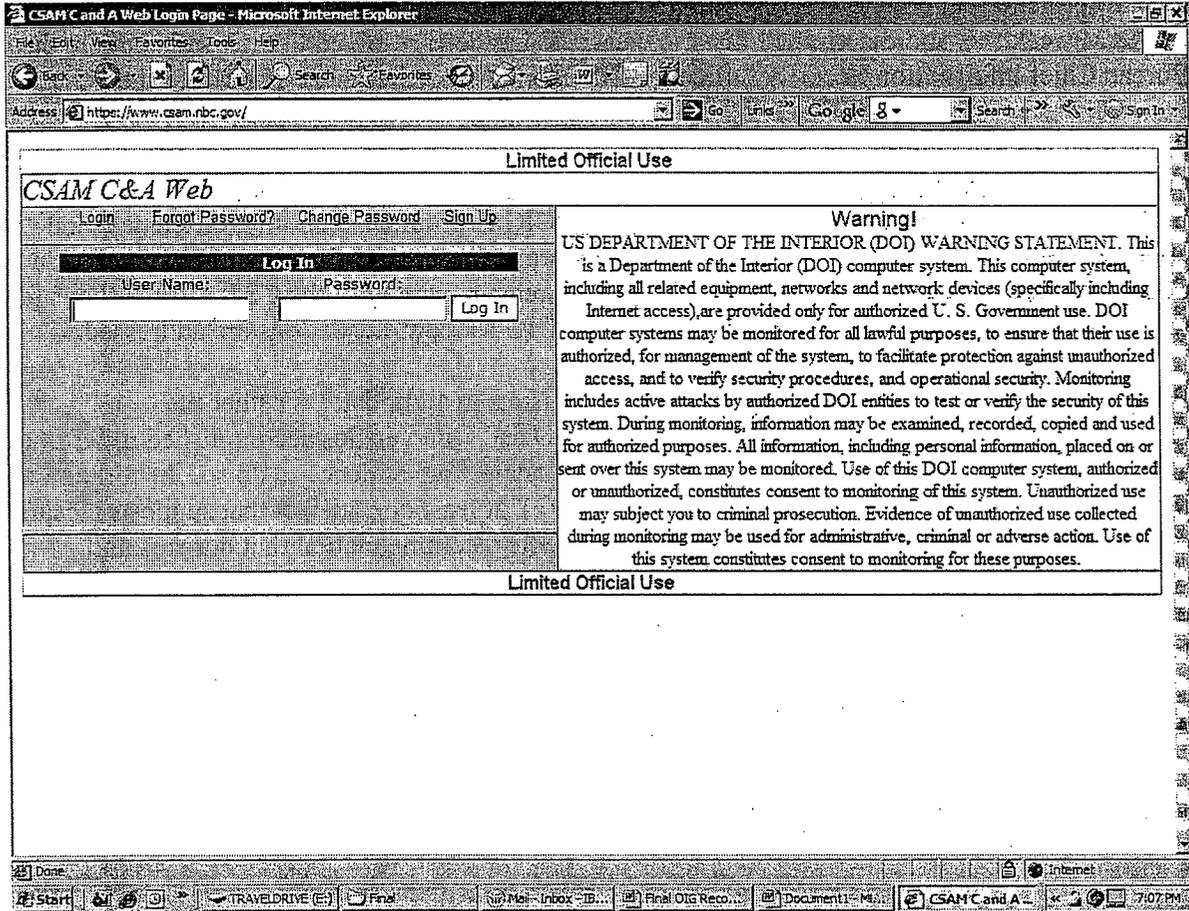
Reporting Schedule

Please refer to Section 2.8.2, Managing and Monitoring Progress.

Creating and Managing POA&Ms

This section will explain how to create and manage program and system POA&Ms as a result of an OIG evaluation in CSAM.

1. To create a program or system POA&M go to: <https://www.csam.nbc.gov>.
2. Enter your User Name and Password and then select **Log in**.



3. Select the Component link and the select the Programs link.

CSAM C&A Web Home - Microsoft Internet Explorer

Address: https://www.csam.nrc.gov/CSAMCentral.aspx

Limited Official Use

CSAM C&A Web User: Davene Barton Log Out Tasks Custom Queries Help

Home SSP Contents Assessment & POAMs **Component Department Maintenance**

Programs
 Dashboard
 FISMA Reports
 Enter Monthly Training Data
 POC Maintenance
 POAM Report (Component SSPs Only)

Component	Recommended Value	Actual Value
Environmental Conservation Online System	No	Yes
Federal Aid Information Management System	Low	Moderate
Migratory Birds Local Area Network	No	Yes
Personal Property Management System	Low	Moderate
	Yes	No

SSP Status Reminders

Accreditations Expiring in 30 days or Late		Accreditations Expiring in 31 - 60 Days		Accreditations Expiring in 61 - 90 days	
SSP	Status Exp Date	SSP	Status Exp Date	SSP	Status Exp Date
OHTA - Accounting Reconciliation Tool	ATO: 2/27/2009	BOR - Central Valley Automated Control System	ATO: 3/31/2009		
OHTA - OHTA Local Area Network	ATO: 2/27/2009	FWS - Data Tracking System	ATO: 3/29/2009		
OS - SIO Alaska Local Area Network	IATO: 7/28/2008	FWS - Environmental Conservation Online System	ATO: 4/15/2009		
OS - Electronic Capital Planning and Investment Control System	IATO: 3/12/2009	NBC - Travel Management System	IATO: 3/31/2009		
USGS - Advanced National Seismic System	ATO: 3/6/2009	OSM - Single Source Coal Reporting System	ATO: 3/30/2009		
USGS - Telecommunications	ATO: 3/6/2009				

POAM Reminders

POAMs Late for Select Org Go

None

Done Start TRAVELDRIVE (E:) Final Mail - Inbox - ID: Final OIG Rec... Document1 - M... CSAM C&A Web 2:07 PM

- Select your bureau/office Project Name and then click the Add POA&M button located on the right side of the screen.

Component Programs Page - Microsoft Internet Explorer

Address: https://www.csam.nrc.gov/POAMS/ComponentPrograms.aspx

Limited Official Use

CSAM C&A Web User: Davene Barton Log Out Tasks Custom Queries Help

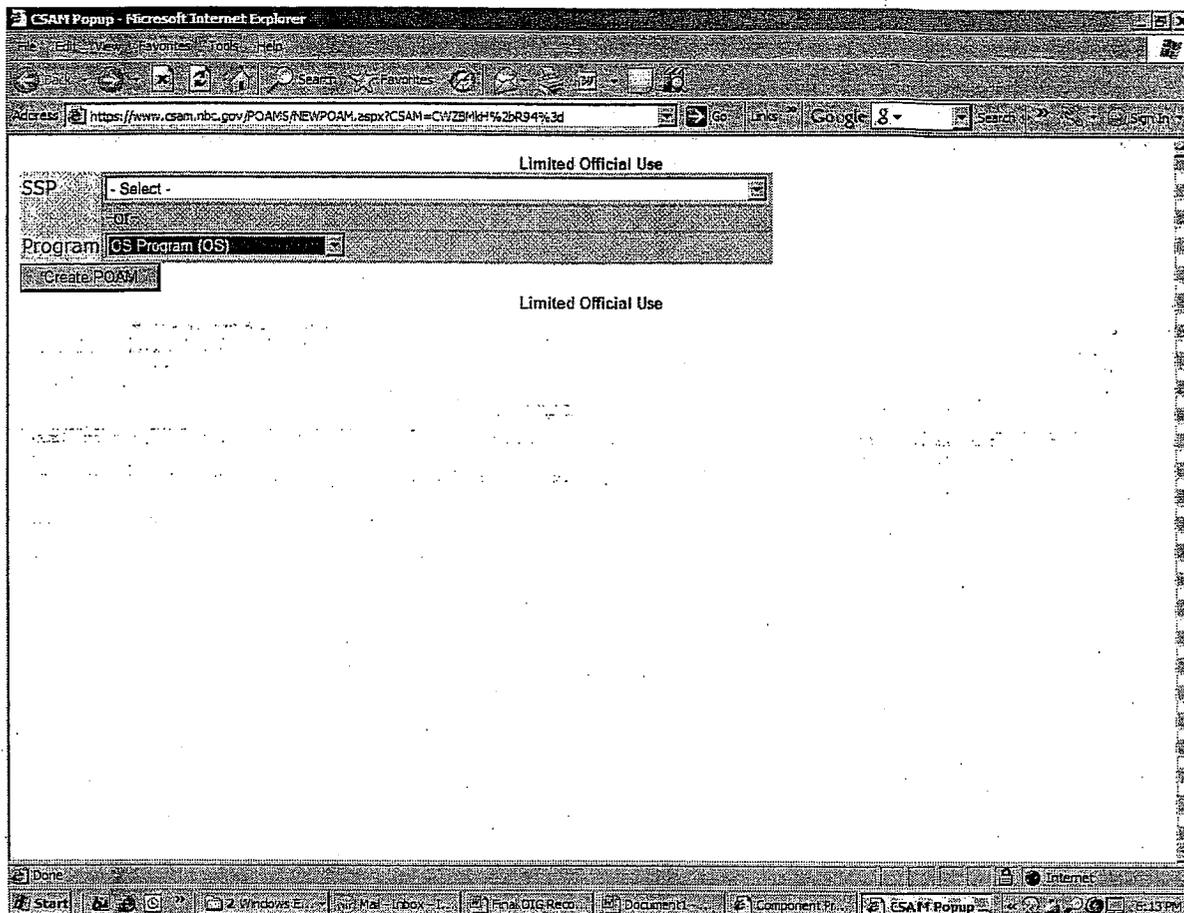
Home SSP Contents POAMs Component Department Maintenance

Component Programs Refresh List Plans of Action and Milestones Add POAM

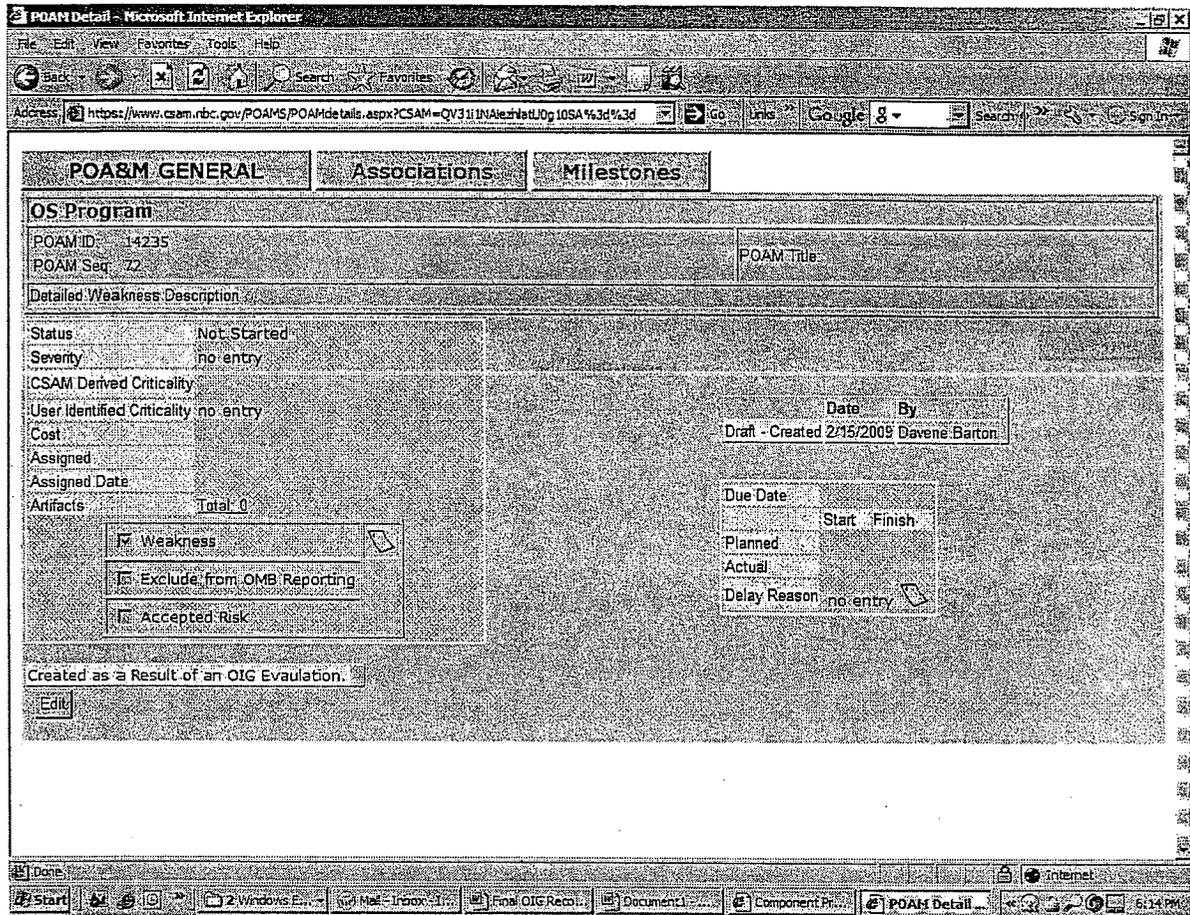
Org	Project Name	Controls	POAM Title	Plan	Actual
				Finish	Finish
BIA	BIA Program	Assess	13963 - ISD-EV-OSS-0013-2008 #11 Design and implement an effective agency-wide Continuous Monitoring progr	9/29/2006	12/31/2009
BLM	BLM Program	Assess			
BOR	BOR Program	Assess			
FWS	FWS Program	Assess	13981 - ISD-EV-OSS-0013-2008 (16) Fully implement and enforce the C&A quality assurance program	8/28/2009	
MMS	MMS Program	Assess			
NBC	NBC Program	Assess			
NPS	NPS Program	Assess	13887 - ISD-EV-OSS-0013-2008 #4 ISD-EV-MOA-0005-2007: OIG Recommendation #2: Complete the mapping	12/31/2008	12/31/2008
OHA	OHA Program	Assess			
OHTA	OHTA Program	Assess			
OS	OS Program	Assess	13869 - Consolidation Of Previous OIG Recommendations (July 15 2008) #5: Routinely monitor end user	6/30/2009	6/30/2009
OSM	OSM Program	Assess			
OST	OST Program	Assess	13870 - Consolidation Of Previous OIG Recommendations (July 15 2008) #6: Implement network access control	6/30/2009	6/30/2009
SOL	SOL Program	Assess			
USGS	USGS Program	Assess	13871 - Consolidation Of Previous OIG Recommendations (July 15 2008) #7: Disable end-user's ability	6/30/2009	6/30/2009
			13872 - Consolidation Of Previous OIG Recommendations (July 15 2008) #2: Implement a personal firewall	6/30/2009	6/30/2009
			13873 - Consolidation Of Previous OIG Recommendations (July 15 2008) #3: Disable end-	6/30/2009	6/30/2009

Start Windows Explorer Mail - Inbox - IBM... Final OIG Recomm... Document1 - Micros... Component Prog... Internet 6:09 PM

5. Select the **Program** or **SSP (system)** name from the pick list and then select **Create POA&M**. (Note: Users will only have access to the systems/program specific to their bureau or office):



6. Select Edit.



The **POA&M ID** is a CSAM generated unique number for each POA&M. This number is unique amongst all system, site and program POA&Ms.

The **POA&M Seq.** is a CSAM generated unique number for each POA&M. This number is unique only within the system, site or program it belongs to. This number is sequentially assigned.

The screenshot shows a web browser window titled "POA&M Detail - Microsoft Internet Explorer". The address bar shows the URL: "https://www.csam.nrc.gov/POAMS/POAMdetails.aspx?CSAM=QV31JINAlczhlaU0g10SA%3d%3d". The page has three tabs: "POA&M GENERAL", "Associations", and "Milestones". The "POA&M GENERAL" tab is selected. The page content includes:

- OS Program** section with fields for POAM ID (14235), POAM Seq (72), and POAM Title.
- A large text area for "Detailed Weakness Description Full Screen Edit".
- A "Status" dropdown menu set to "Not Started".
- A "Severity" dropdown menu set to "Other Weakness".
- A "CSAM Derived Criticality" dropdown menu.
- A "User" field.
- An "Identified" dropdown menu set to "Low".
- A "Cost" field.
- An "Assigned" dropdown menu set to "- Select POC -".
- An "Assigned Date" field.
- An "Artifacts Total" field set to 0.
- A "Draft" status indicator with "Created 2/15/2009" and "By Davene Barton".
- A "- Status Change Request Options -" dropdown menu and a "Submit" button.
- A table with columns: Due Date, Date, Start, Planned, Actual, Auto Schedule, and Finish. All values are TBD.

7. Enter **POA&M Title**. Enter the OIG report evaluation number the recommendation number and a brief description of the weakness Select **Edit** Select **Edit**.
8. Enter **Detailed Weakness Description**. Enter the detailed weakness description in the text box using the exact language identified in the OIG report evaluation. (Note: If the OIG recommendation has been identified in multiple reports, open only one POA&M and list all report evaluation numbers and recommendation numbers).
9. Enter **Severity** by clicking the drop- down menu and choosing the applicable option.
10. **CSAM Derived Criticality**. CSAM automatically ranks the criticality of a POA&M when the vulnerability is associated at the Control or Expected Results level and is unaware of the operating environment of the system (i.e., is not aware of any mitigating/compensating controls that would justify any lower risk rating – e.g., a vulnerable port/service might have an initial risk rating of high but when taking into consideration an external firewall that prevents any other system from accessing the vulnerable port/service the user identified risk level might be adjusted to medium or low).

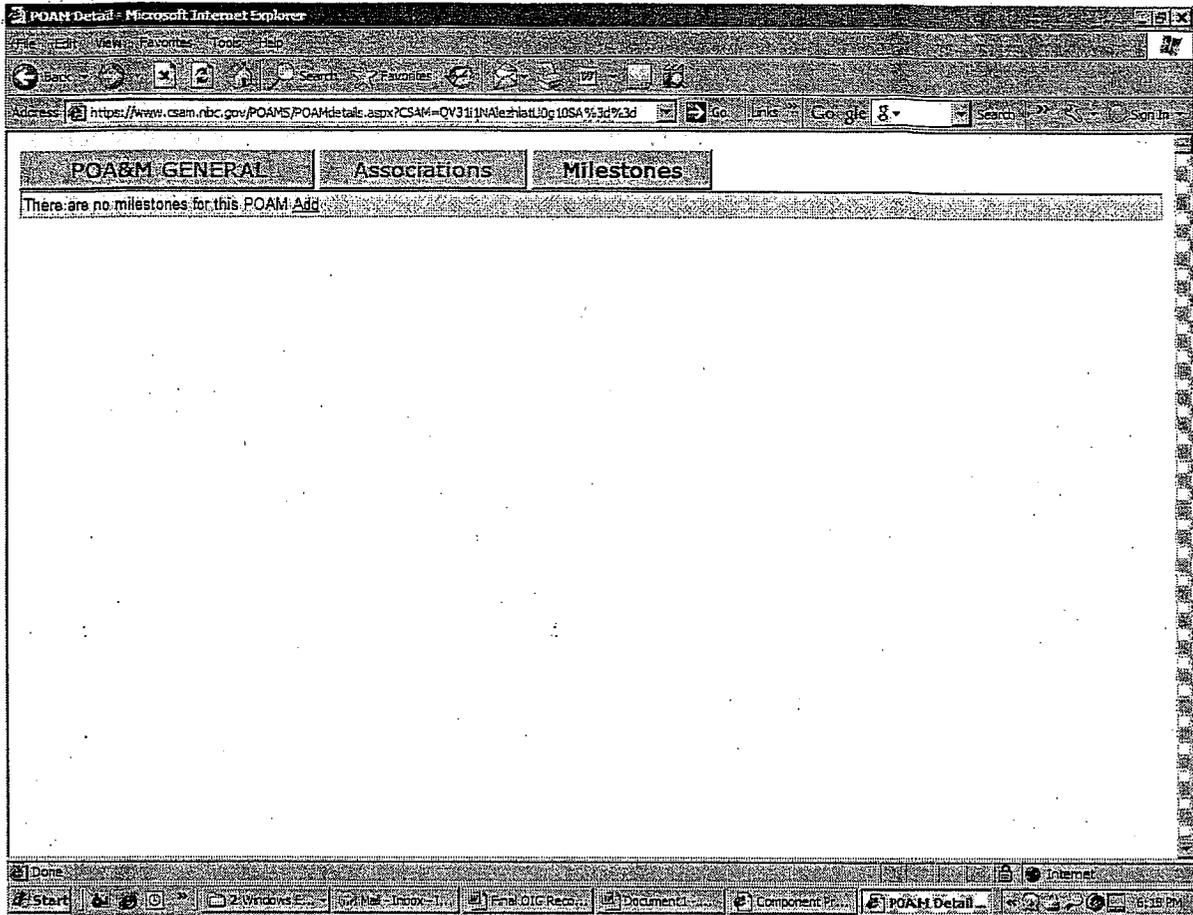
The **CSAM Derived Criticality** value is dynamically updated as the associated control implementation status changes. In the event the vulnerability is not associated at the

control or expected result level, the user identified criticality level must be populated. An example of this may be Program related vulnerabilities.

11. Select the **User Identified Criticality** of the POA&M from the pick list. Using data from a user defined risk assessment process, enter appropriate the criticality level. (Note: The User Identified Criticality level is the "official criticality level" to the extent that it is selected/identified as instructed by this POA&M Process Standard. If it is not adjusted by the user then the "official criticality level" would default to the "CSAM Derived Criticality".
12. Enter the **Cost** information. POA&M cost can be captured and associated with the POA&M, providing visibility on several other CSAM screens. This capability enables IT Security Specialists and management to make credible, risk-based decisions with regard to the operation and use of information systems.
13. Enter **Assigned POC**. This assignment is made from a drop down table of POCs for which CSAM contains contact information online.
14. Enter the **Due Date** also known as the Schedule Completion Date (SCD). This date is the key date that will be locked-down as the baseline, once the POA&M is approved. While in Draft POA&M status, this value can be changed. The user can also enter dates directly into individual fields. Auto-scheduler sets the **Due Date, Planned Start** and **Planned Finish** dates, however, the user must enter the **Actual Start** and **Actual Finish** dates manually.
15. Select **Yes** from the **Created as a Result of an OIG Evaluation** pick list, enter the **Source of Weakness**. When entering the source of weakness information bureaus/offices must include the title of the report, the report number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness. Click Save.

sources of weaknesses by including the auditing entity, the title of the report, the report number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness. It is anticipated that this interim approach will enable Interior to more easily migrate the information in the temporary UDA fields to the more permanent fields following DOJ's implementation of the change request (expected to take at least six months or longer – DOJ is unable to provide any specific commitments and/or dates at this time).

16 Select the Milestones tab:



The key milestones associated with each corrective action should be identified on each POA&M. Each weakness must have one or more associated milestones. Milestones should define the major steps that will be performed to complete the corrective action. If there is more than one milestone, list and number each milestone in the order they should be executed. For example, one set of milestones for a weakness such as, "Identification and authentication are not adequate for the level of security controls required for this system" might be:

- 1) Evaluate methods for strengthening identification and authentication.
- 2) Recommend solution and obtain approval.
- 3) Develop procedures to standardize accepted identification and authentication process.
- 4) Design identification and authentication solution.
- 5) Build identification and authentication solution.
- 6) Test identification and authentication solution.
- 7) Deploy identification and authentication solution and implement supporting process.

Milestones might also include more specific aspects related to the technical solution (e.g. implement two-factor authentication), and management and operational controls related to the steps for implementing supporting business practices and procedures where additional security control requirements are known or anticipated.

The description of each milestone must be detailed enough so that an independent reviewer will understand the planned corrective action and determine whether the corrective action is adequate and appropriate and will result in the weakness being corrected or its associated risk mitigated to a level acceptable to the AO. Sensitive information can be included as needed for the description since the entire POA&M is a sensitive but unclassified document.

Milestones should start with planned remediation actions, show progression through remediation and/or must be updated periodically or as remediation actions occur.

Milestones should always end in a statement clearly indicating completed remediation action; Entries of TBD, N/A, and similar responses indicating future tense, proposed or intended actions are not compliant.

17. Select **Add** to add a milestone and enter required dates. At least one milestone must be added before a POA&M can be approved.

18. Select **Update** to save the entry.

The screenshot shows a Microsoft Internet Explorer browser window displaying the 'POA&M Detail' page. The browser's address bar shows the URL: <https://www.csam.nrc.gov/POAMS/POAMdetails.aspx?CSAM=QV3J1NA1ezh1aU0g10SA%3d%3d>. The page has three tabs: 'POA&M GENERAL', 'Associations', and 'Milestones'. The 'Milestones' tab is active, showing a table with the following data:

Add	Milestone	Due	Planned Start	Planned Finish	Actual Start	Actual Finish
	Milestone Description	2/19/2009	2/23/2009	2/24/2009	2/15/2009	

Below the table, there is an 'Add' form with the following fields:

- Milestone Description:** A large text area for entering the milestone description.
- Assigned To:** A dropdown menu currently showing 'Davene Barton'.

At the bottom of the form, there are 'Update' and 'Cancel' buttons. The Windows taskbar at the bottom of the screen shows the 'Start' button, several open applications (Windows Explorer, Mail, Internet Explorer, File, OIG Rec., Documents, Component), and the 'POA&M Detail' application. The system clock shows 4:19 PM.

19. Select the POA&M General tab and then select Edit.

POAM Detail - Microsoft Internet Explorer

Address: https://www.csam.nbc.gov/POAMS/POAMdetails.aspx?CSAM=QV311UNALEZHLTJ0g10SA%3d%3d

POA&M GENERAL Associations Milestones

OS Program

POAM ID: 14235 POAM Title: _____
 POAM Seq: 72 OIG Evaluation(Recommendation=) Brief Description: _____

Detailed Weakness/Description Full Screen/Edit

Description

Status: Not Started

Severity: Other Weakness

CSAM

Derived

Criticality

User

Identified: Low

Criticality

Cost: 10

Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438

Assigned Date

Artifacts Total: 0

Date By

Draft - Created 2/15/2009 Davene Barton

Status Change Request Options - Submit

Due Date: 3/17/2009 Auto Schedule: 20 Days

Start: _____ Finish: _____

Planned: 2/15/2009 3/17/2009

Actual: TBD TBD

Done

Start 2 Windows E... Mail - Inbox - 1... Final OIG Rec... Document... Component Pr... POAM Detail... 6:23 PM

20. Select **Draft – Approval Requested** from the **Status Change Request Options** pick list and then click **Submit**.

The POA&M Approval Status options are as follows:

Draft Created: Each POA&M automatically starts in this state. A POA&M in this state can be deleted by any user who can edit the POA&M

Draft Approve Requested: When the key POA&M information has been entered and finalized, the user responsible for maintaining the POA&M selects this status to request approval. At least one milestone must have been entered before this event can be selected. Requires permission POAMEDIT.

POAM Approved: The user responsible for reviewing POAM Approval requests selects this status to indicate that the request has been approved. The user responsible for the POA&M can continue carrying out the actions and milestones associated with the POA&M. Once approved, the POA&M Title, Detailed Weakness Description, and Due Date fields are locked in read-only mode for regular users. Requires permission POAMAPPR or POAMAPSSP.

POAM Approval Denied: The user responsible for reviewing POAM Approval requests selects this status to indicate that the request has been denied. The user

responsible for the POA&M can then make changes and resubmit the approval request. Requires permission POAMAPPR or POAMAPSSP.

POAM Auto Approved: The POA&M will automatically enter this state if it has not already been approved through the manual event process after 90 days from creation. The POA&M Title, Detailed Weakness Description, and Due Date fields are locked in read-only mode for regular users, with the exception that the Due Date field may be edited once if it was NULL when the POA&M was Auto-Approved.

POAM Cancellation Requested: The user responsible for maintaining the POA&M can request cancellation if the POA&M has been approved and is still open. Typically this is done if the POA&M is a duplicate or if the requirement is no longer valid. Requires permission POAMCANCEL.

POAM Close Requested: The user responsible for maintaining the POA&M can request close if the POA&M has been approved and is still open. Typically this is done when after the POA&M actions and milestones have been carried out to completion. The POA&M Actual Start and Actual Finish dates must be populated before this event can be selected. Requires permission POAMCLOSE.

Cancel Approved: The user responsible for reviewing POAM Cancellation requests selects this status to indicate that the request has been approved. The POA&M status changes to Cancelled and no further actions are required on the POA&M. Requires permission POAMAPCANCEL.

Cancel Denied: The user responsible for reviewing POAM Cancellation requests selects this status to indicate that the request has been denied. The user responsible for the POA&M can then make changes and resubmit the cancellation request with a new justification, or work the actions and milestones to closure. Requires permission POAMAPCANCEL.

21. To approve entry of the POA&M, From the POA&M General tab select **Edit, POA&M Approved** from the Status Change Request Options, provide comments and then click **Submit**.

POA&M GENERAL Associations Milestones

OS Program

POAM ID: 14235 POAM Title: _____
 POAM Seq: 72 OIG Evaluation(Recommendation=) Brief Description: _____

Detailed Weakness Description Full Screen Edit

Description

Status: Not Started

Severity: Other Weakness

CSAM

Derived

Criticality

Use

Identified: Low

Criticality

Cost: 10

Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438

Assigned Date: 2/15/2009

Artifacts Total: 0

Draft	Created	Date	By
Draft - Created	2/15/2009		Davene Barton
Draft - Approval Requested	2/15/2009		Davene Barton
Draft - Approval Requested	2/15/2009		Davene Barton

-Approval Options- Submit

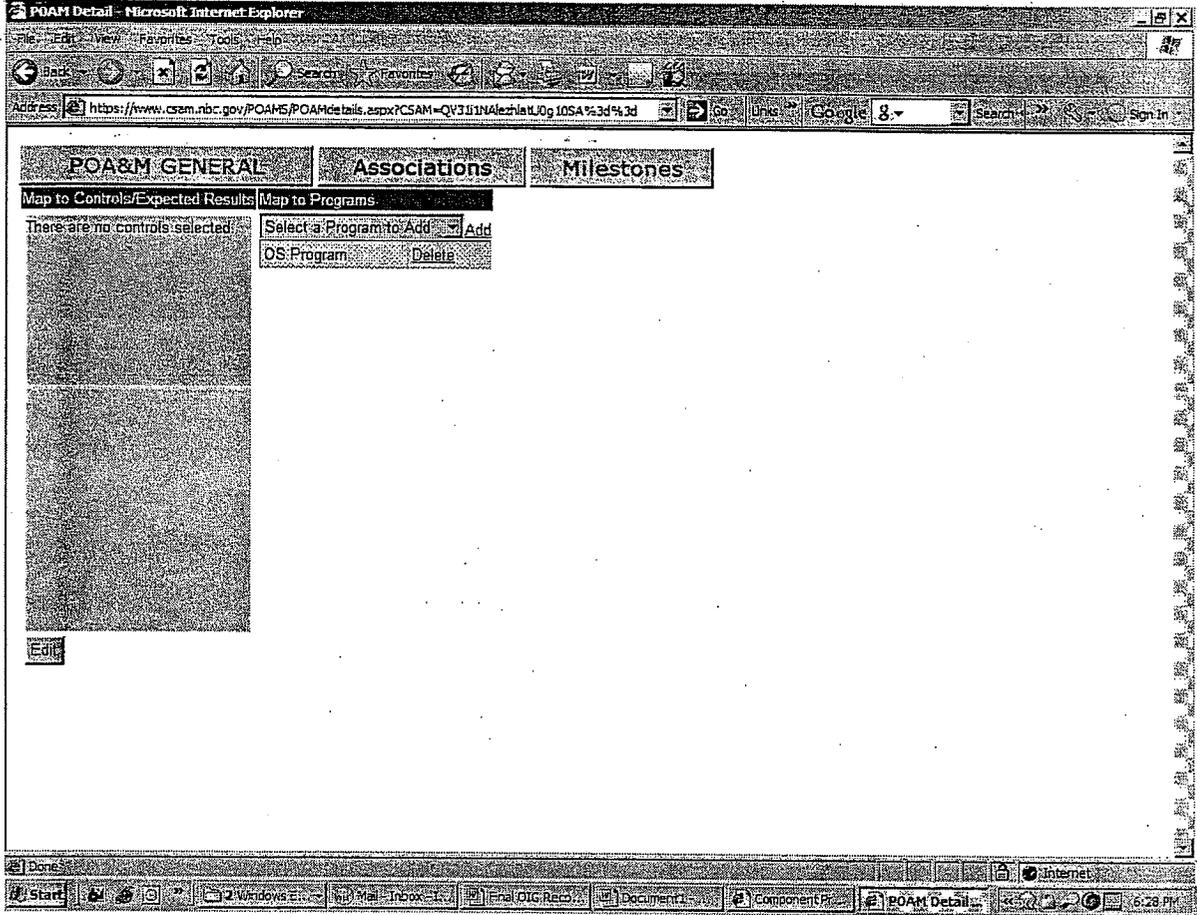
-Approval Options-

POA&M Approved

POA&M Approval Denied

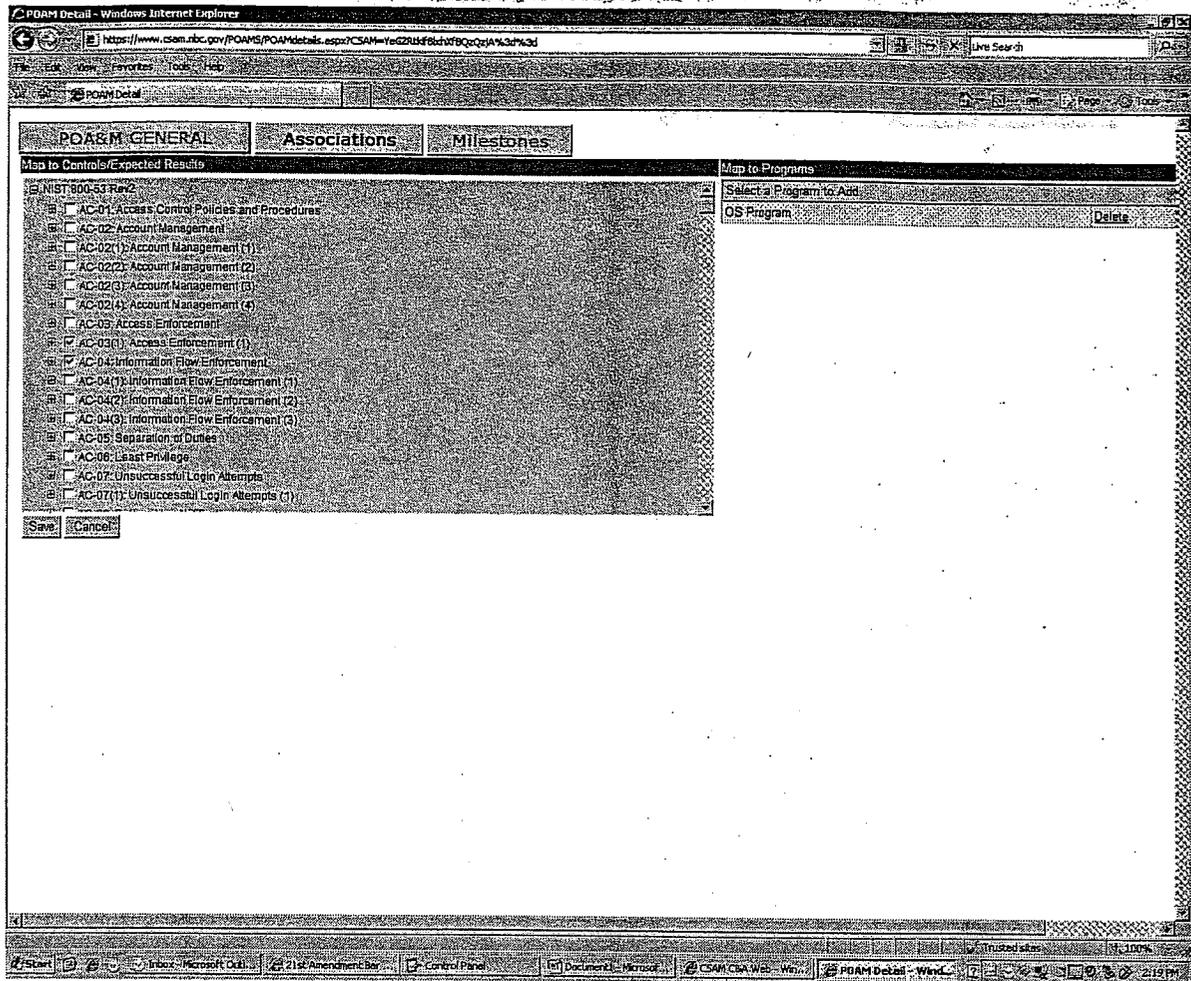
Due Date: 3/17/2009 Auto Schedule: Select a Schedule

22. Select the Associations tab to tag multiple controls and expected results to Programs.



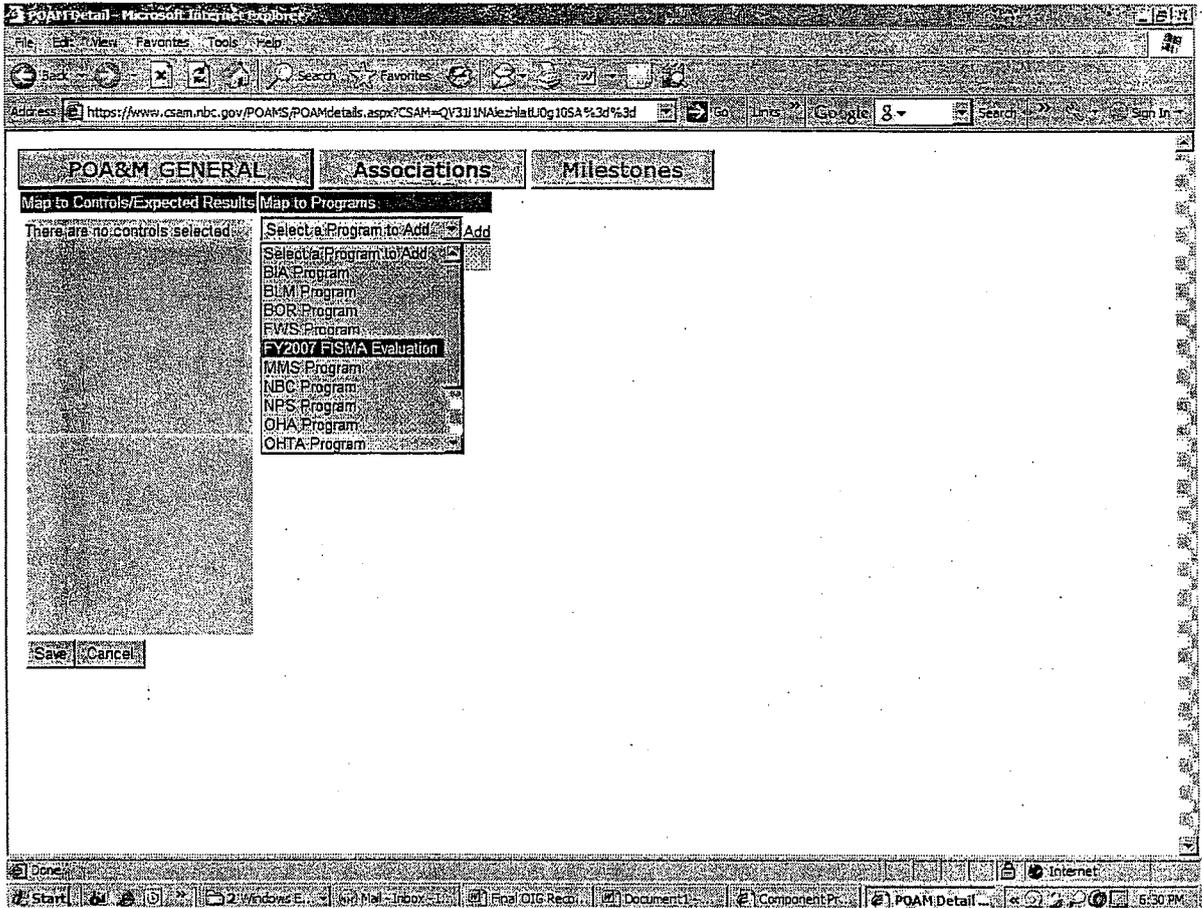
23. Select **Edit**.

24. Select applicable controls.



25. Select a Program to add and then click **Add**. (Note: Please map POA&Ms created as a result of an OIG evaluation to the appropriate "FY200X FISMA Evaluation" program and then click **Save**.)

26. Select the **POA&M General** Tab and exit the application. This completes the POA&M creation work flow process.



27. To request closure of a POA&M, select the Component link and then scroll down and select the Programs link.

Limited Official Use

CSAM C&A Web | User: Davene Barton | Log Out | Tasks | Custom Queries | Help

Home | SSP | Contents | Assessments | POAMs | Reports | Component | Department | Maintenance

The following is:

- Programs
- Dashboard
- FISMA Reports
- Enter Monthly Training Data
- POC Maintenance
- POAM Report (Component SSPs Only)

Current P2M Selection Factors	Recommended Value	Actual Value
	No	Yes
	Low	Moderate
	No	Yes
	Low	Moderate
	Yes	No

SSP Status Reminders

Accreditations Expiring in 30 days or Late		Accreditations Expiring in 31 - 60 Days		Accreditations Expiring in 61 - 90 days
SSP	Status Exp Date	SSP	Status Exp Date	None
OHTA - Accounting Reconciliation Tool	ATO: 2/27/2009	BOR - Central Valley Automated Control System	ATO: 3/31/2009	
OHTA - OHTA Local Area Network	ATO: 2/27/2009	FWS - Data Tracking System	ATO: 3/29/2009	
OS - SIO Alaska Local Area Network	IATO: 7/28/2008	FWS - Environmental Conservation Online System	ATO: 4/15/2009	
OS - Electronic Capital Planning and Investment Control System	IATO: 3/12/2009	NEC - Travel Management System	ATO: 3/31/2009	
USGS - Advanced National Seismic System	ATO: 3/5/2009	OSM - Single Source Coal Reporting System	ATO: 3/30/2009	
USGS - Telecommunications	ATO: 3/6/2009			

POAM Reminders

POAMs: Late | for: Select Org | Go

None

28. Select the bureau/office Project Name and then select the POA&M that you would like to close located on the right side of the screen under POA&M Title.

Component Programs Page - Microsoft Internet Explorer

Address: https://www.csam.nrc.gov/POAMS/ComponentPrograms.aspx

Limited Official Use

CSAM C&A Web User: Davene Barton Log Out Tasks Custom Queries Help

Home SSP Contents Assessments POAMs Reports Component Department Maintenance

Component Programs Refresh Lists Plans of Action and Milestones Add POAM

Org	Project Name	Controls	POAM Title	Date	Planned Finish	Actual Finish
BIA	BIA Program	Assess	14235 - OIG Evaluation (Recommendation #1: Brief	3/17/2009	3/17/2009	
BLM	BLM Program	Assess	Description:			
BOR	BOR Program	Assess	1996 (Click to View the POAM Details): #1 Design and	9/29/2006	12/31/2009	
FWS	FWS Program	Assess	implement an effective agency-wide Continuous			
MMS	MMS Program	Assess	Monitoring program			
NBC	NBC Program	Assess	13981 - ISD-EV-OSS-0013-2008: #6: Fully	8/28/2009		
NPS	NPS Program	Assess	implement and enforce the C&A quality assurance			
OHA	OHA Program	Assess	program			
OHTA	OHTA Program	Assess	13887 - ISD-EV-OSS-0013-2008: #4: ISD-EV-	12/31/2008	12/31/2008	
OS	OS Program	Assess	MOA-0005-2007: OIG Recommendation			
OSM	OSM Program	Assess	#2: Complete the mapping			
OST	OST Program	Assess	13869 - Consolidation Of Previous OIG	6/30/2009	6/30/2009	
SOL	SOL Program	Assess	Recommendations (July 15 2008): #5: Routinely			
USGS	USGS Program	Assess	monitor end user			
			13870 - Consolidation Of Previous OIG	6/30/2009	6/30/2009	
			Recommendations July 15 2008: #6: Implement			
			network access control			
			13871 - Consolidation Of Previous OIG	6/30/2009	6/30/2009	
			Recommendations (July 15 2008): #7: Disable			
			and user's ability			
			13872 - Consolidation Of Previous OIG	6/30/2009	6/30/2009	
			Recommendations (July 15 2008): #2: Implement a			
			personal firewall...			

https://www.csam.nrc.gov/POAMS/POAMDetails.aspx?CSAM=003311NA&mitt=0010CSA%3d%3d

Start Windows Explorer Mail - Inbox - IBM... Final OIG Recomm... Documents - Micro... Component Prog... 6:40 PM

29. Select Edit.

POA&M Detail - Microsoft Internet Explorer

https://www.osam.nrc.gov/POA&M/POA&MDetails.aspx?CSAM=QV331NAIezh1tU0g10SA%3d%3d

POA&M GENERAL Associations Milestones

OS Program

POA&M ID: 114235 POA&M Title: OIG Evaluation (Recommendation) - Brief Description

POA&M Seq: 72

Detailed Weakness Description

Description

Status	Planned/Pending
Severity	Other Weakness
CSAM Derived Criticality	
User Identified Criticality	Low
Cost	10
Assigned	Davene Barton
Assigned Date	2/15/2009
Artifacts	Total: 0

Date	By
Draft - Created	2/15/2009 Davene Barton
Draft - Approval Requested	2/15/2009 Davene Barton
Draft - Approval Requested	2/15/2009 Davene Barton
POAM Approved	2/15/2009 Davene Barton

Due Date	3/17/2009
Planned	Start: 2/15/2009 Finish: 3/17/2009
Actual	
Delay Reason	no entry

Weakness

Exclude from OMB Reporting

Accepted Risk

Created as a Result of an OIG Evaluation: Yes

[Edit](#)

Windows Explorer Mail Inbox Final OIG Recl... Document1... Component Pr... POA&M Detail... Start

30. Select **POA&M Close Requested**, from the **Status Change Request Options**, provide comments in the text box below and then click **Submit**.

POA&M GENERAL **Associations** **Milestones**

OS Program

POAM ID: 14235 POAM Title: _____
 POAM Seq: 72 OIG Evaluation(Recommendation=) Brief Description: _____

Detailed Weakness Description Full Screen Edit

Description: _____

Status: Planned/Pending
 Severity: Other Weakness
 CSAM Derived Criticality: _____
 User Identified: Low
 Criticality: _____
 Cost: 10
 Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438
 Assigned Date: 2/15/2009
 Artifacts Total: 0

Date	By
Draft - Created	2/15/2009 Davene Barton
Draft - Approval Requested	2/15/2009 Davene Barton
Draft - Approval Requested	2/15/2009 Davene Barton
POAM Approved	2/15/2009 Davene Barton

Status Change Request Options Sub

- Status Change Request Options-
- Status Change Request Options-
- POAM Cancellation Requested
- POAM Close Requested**

Due Date: 3/17/2009 Auto Schedule

Note: After a POA&M weakness has been closed there are limited capabilities to modify them. Please ensure that newly created POA&Ms are in compliance with this standard. All POA&M weaknesses that are closed but are found to be non-compliant must be corrected or re-created with a reference to the original POA&M ID number in the POA&M Title field. The re-created (new) POA&M must reference the original POA&M ID number in the "POA&M Title" field. Additionally, the original (old) POA&M must reference the re-created POA&M ID number in the "POA&M Title" field.

31. Select the paper icon located next to Weakness, Select **Add Comment**, enter the corrective action(s) in the comment field and select **Update**.

POAM Detail: Microsoft Internet Explorer

Address: https://www.csem.nrc.gov/POAMS/POAMDetails.aspx?CSAM=QV31JNAZehiaUJog10SA%3d%3d

Detailed Weakness Description Full Screen Edit

Description

Status: Planned/Pending

Severity: Other Weakness

CSAM

Derived

Criticality

User

Identified: Low

Criticality

Cost: 10

Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438

Assigned Date: 2/15/2009

Artifacts: Total: 0

Weakness

Exclude from OMB Reporting

Accepted Risk

	Date	By
Draft - Created	2/15/2009	Davene Barton
Draft - Approval Requested	2/15/2009	Davene Barton
Draft - Approval Requested	2/15/2009	Davene Barton
POAM Approved	2/15/2009	Davene Barton

POAM Close Requested

Close.

Due Date	Start	Finish	Auto Schedule
3/17/2009	2/15/2009	3/17/2009	Select a Schedule
	2/15/2009	2/15/2009	

Delay Reason: -No Selection-

Taskbar: Start, Windows Explorer, Mail - Inbox - IB..., Outlook Recor..., Document..., Component Pro..., POAMDetail, 6:45 PM

32. Click on the Total icon, to the right of Artifacts and upload artifacts such as Weakness Completion Verification Forms (WCVFs), screenshots, memorandum signature pages and other relevant evidentiary artifacts that clearly demonstrate successful resolution of the weakness.

POAM Detail - Microsoft Internet Explorer

Address: <https://www.csam.nbc.gov/POAMS/POAMdetails.aspx?CSAM=QV3J1N4AezhlaU0g10SA%3d%3d>

Detailed Weakness: Description Full Screen Edit

Description

Status: Planned/Pending
 Severity: Other Weakness

CSAM Derived Criticality

User Identified: Low
 Criticality

Cost: 10

Assigned: Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438
 Assigned Date: 2/15/2009

Artifacts Total: 1

Weakness
 Exclude from OMB Reporting
 Accepted Risk

Date	By
Draft - Created	2/15/2009 Davene Barton
Draft - Approval Requested	2/15/2009 Davene Barton
Draft - Approval Requested	2/15/2009 Davene Barton
POAM Approved	2/15/2009 Davene Barton

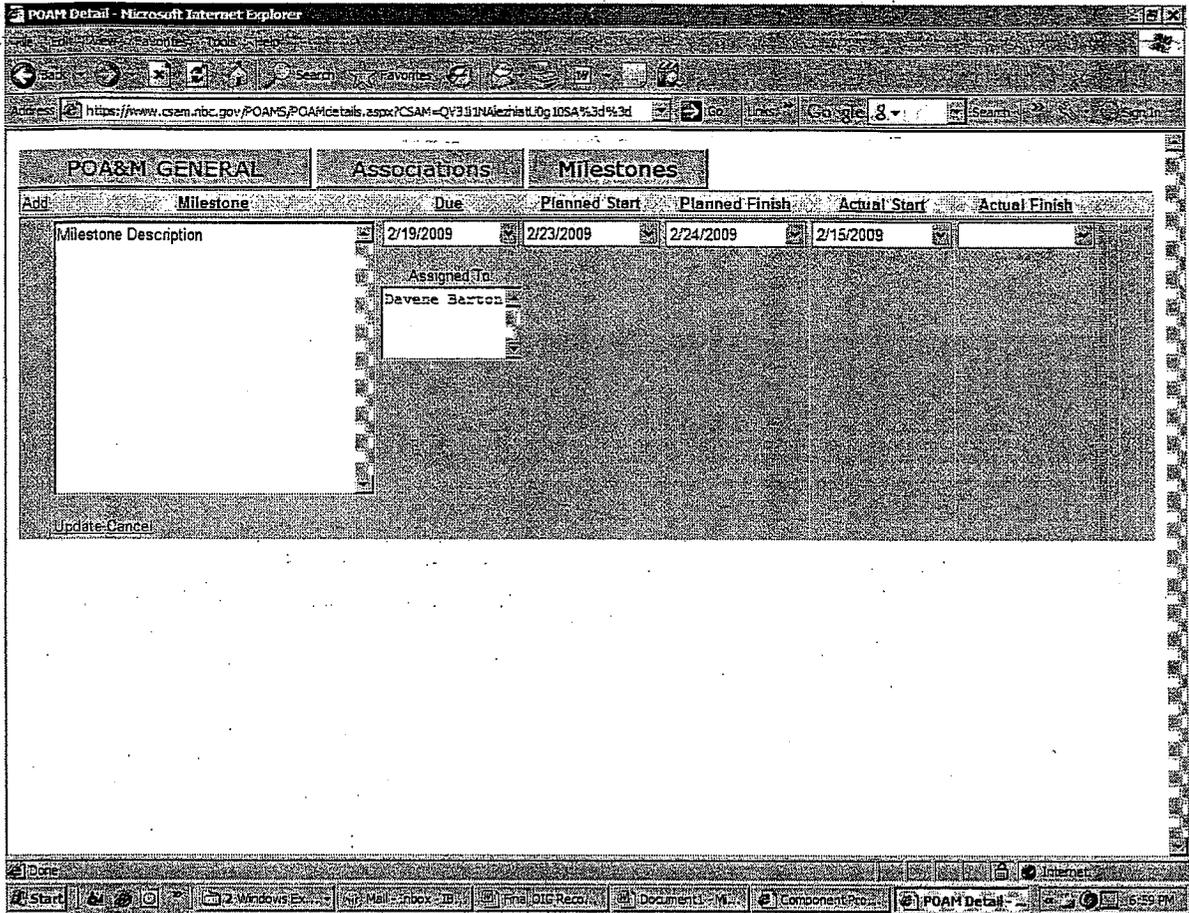
POAM Close Requested: [Dropdown] Sub

Close:

Due Date	Start	Finish
3/17/2009	2/15/2009	3/17/2009
	2/15/2009	2/15/2009

Delay Reason: -No Selection-

33. Select the Milestones tab and then click Add.



34. Enter the milestone **Actual Finish** date.

35. Select **Update** to save the entry, select the **POA&M General Tab** and exit the application.

The CSD will generate a custom query report no less than quarterly on all POA&Ms that have a status of **POA&M Close Requested** and will re-evaluate the effectiveness of corrective actions. Once the CSD has determined that the weakness has been resolved to their satisfaction, the Bureau Chief Information Security Officer (BCISO) will be notified via e-mail from the CSD that the weakness has been successfully resolved.

Upon receipt of the e-mail from the CSD, return to the POA&M module in CSAM.

36. Select **Close Approved** from the **Status Change Request Options**, provide comments and then click **Submit**.

POAM Detail - Microsoft Internet Explorer

Address: <https://www.csam.nbc.gov/POAMS/POAMdetails.aspx?CSAM=QV31JfNAezrlatU0g10SA%3d%3d>

POA&M GENERAL Associations Milestones

OS Program

POAM ID: 14235 POAM Title:
 POAM Seq: 72

Detailed Weakness Description Full Screen Edit

Description:

Status	Date	By
Draft - Created	2/15/2009	Davene Barton
Draft - Approval Requested	2/15/2009	Davene Barton
Draft - Approval Requested	2/15/2009	Davene Barton
POAM Approved	2/15/2009	Davene Barton
POAM Close Requested	2/15/2009	Davene Barton

Status:
 Severity:
 CSAM:
 Derived:
 Criticality:
 User:
 Identified:
 Criticality:
 Cost:
 Assigned:
 Assigned Date:
 Artifacts: Total:

-Status Change Request Options-

-Status Change Request Options-

- Close Approved
- Close Denied

Start | 2 Windows Ex... | Mail - Inbox - IB... | Final OIG Rec... | Document1 - M... | Component Pro... | POAM Detail... | 7:03 PM

37. Enter the Actual Finish date and click Save to close the POA&M. The status will change from In Progress, Delayed or Ongoing to Completed.

POA&M GENERAL Associations Milestones

OS Program

POAM ID: 14235 POAM Title: OIG Evaluation (Recommendation) Brief Description

POAM Seq: 72

Detailed Weakness Description

Description

Status: Completed
 Severity: Other Weakness

CSAM Derived Criticality

User Identified Criticality: Low

Cost: 110

Assigned: Davene Barton

Assigned Date: 2/15/2009

Artifacts: Total: 0

Weakness

Exclude from OMB Reporting

Accepted Risk

Created as a Result of an OIG Evaluation: Yes

	Date	By
Draft - Created	2/15/2009	Davene Barton
Draft - Approval Requested	2/15/2009	Davene Barton
Draft - Approval Requested	2/15/2009	Davene Barton
POAM Approved	2/15/2009	Davene Barton
POAM Close Requested	2/15/2009	Davene Barton
Close Approved	2/15/2009	Davene Barton

Due Date: 3/17/2009

	Start	Finish
Planned	2/15/2009	3/17/2009
Actual	2/15/2009	2/15/2009

Delay Reason: no entry

Appendix G: CSAM Account Management Procedures

Purpose

The purpose of this document is to provide guidance for account management for the Cyber Security Assessment and Management (CSAM) C&A Web application henceforth referred to as "CSAM". Generally, people think of this as primarily covering the creation or changing of new user accounts (Government, contractor, regular and privileged users). However, that is just the beginning of account management. This document and the associated references also address the disabling of inactive or retired accounts and the annual recertification of accounts. Additionally, this document and its associated references also cover the processes of adding, deleting, and changing systems, components, and subcomponents to CSAM.

Scope and Applicability

The following procedures apply to all DOI CSAM application users, regardless of where they may be located.

Roles and Responsibilities

Account Manager Approving Official

The Account Manager Approving Official (AMAO) is the designated individual with authority to appoint the bureau or office Account Manager (AM). The AMAO must be the Bureau Chief Information Security Officer (BCISO), a higher official, or their duly authorized Representative as established by bureau or office BCISO in consultation with the bureau or office Chief Information Officer (CIO). The designation of all account representatives must be in writing. E-mail or signed fax is acceptable.

Account Approving Official

The Account Approving Official (AAO) is the designated individual authorized to request account creation, deletion, and modification for their respective users and/or systems. The AAO must be the system's owner, a higher official, or their duly authorized representative as established by bureau or office BCISO in consultation with the bureau or office (CIO). AAO authorization (signature, signed fax, or email is acceptable) is required on all requests prior to the requested actions being fulfilled.

Account Manager

The Account Manager (AM) is the designated individual with primary responsibilities of handling account requests and other administrative actions related to the respective bureau or office users and systems under their purview (e.g., activate, edit, and delete user accounts). Also provides ability to assign users to System Security Plans (SSP). The designation of the bureau or

office Account Manager must be in writing by the AAO. The AM must obtain written approval from the AAO before user accounts are created, deleted or modified.

Administrator

The administrator is granted unrestricted rights to the entire system. The administrator has the ability to administer advanced functions, including updates to pick lists and templates.

Audit Log Reviewer

The Audit Log Reviewer is responsible for reviewing audit logs.

Author

The Author is the designated individual with the ability to update narratives and appendices that have been assigned. The Author can also update control-level fields (e.g. compliance description, test results, POA&Ms) for those controls that have been assigned, however, the Author does not have the ability to update most fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping).

Authorizing Official

The Authorizing Official (AO) is responsible for conducting the quarterly review of systems under their purview prior to the submission of POA&Ms for OMB reporting; and reviewing all residual risk recommended for acceptance by the system owner, user representative, system manager, or BCISO.

Authorizing Official Designated Representative

The Authorizing Official Designated representative may be called upon to review the quarterly POA&Ms and obtain the authorizing official's signature on acceptance of any residual risks.

Bureau or Office Account Manager

The bureau or office Account Manager (AM) is the designated individual with primary responsibilities for handling account requests and other administrative actions related to the respective bureau or office users and systems under their purview (e.g., activate, edit, and delete user accounts. Also provides ability to assign users to SSPs). The designation of the bureau or office Account Manager must be in writing by the AAO. The AM must obtain written approval from the AAO before user accounts are created, deleted or modified.

Bureau or Office Chief Information Security Officer

The bureau or office Chief Information Security Officer (BCISO) is responsible for reviewing corrective actions for their respective bureau or office to ensure that each corrective action is an

effective and appropriate mitigation solution for its targeted weakness. Also, the BCISO is responsible for verifying the completion status of system security weaknesses reported in POA&Ms.

Bureau and Office Lead

The designated bureau or office representative responsible for component programs, component-level report card(s), and component FISMA reports.

Certification and Accreditation (C&A) Manager

The C&A manager shall be responsible to the bureau for ensuring adequate planning and compliance with respect to the certification and accreditation and IT security requirements, standards and guidelines issued by the Office of Management and Budget (OMB), NIST, and DOI.

Certification Agent

The certification agent is an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Compliance Team

The compliance team reviews and evaluates the method of implementation and effectiveness of the bureau and office IT security programs within DOI.

Control Author

The Control Author is the designated DOI-wide representative with the ability to author security control content.

Department Lead

The designated DOI-wide representative responsible for activating, editing, and deleting bureau and office user accounts.

Information Owner

The information owner is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information System Owner

The Information System Owner (ISO) is responsible for updating the C&A package with documentation on completed POA&M items (append approved verification form.); and in coordination with the BCISO, the ISO is responsible for providing routine reviews and status reports on corrective actions to the bureau CIO and AO, no less than quarterly.

Information System Security Officer

Information System Security Officer

The ISSO is responsible for ensuring the appropriate operational security posture is maintained for an information system or program. In coordination with the ISO, the ISSO plays an active role in developing and updating the system security plan (SSP) as well as in managing and controlling changes to the system and assessing the security impact of those changes.

OCIO Reviewer

The OCIO reviewer is responsible for performing OCIO reviews for assigned SSPs and controls.

OIG Reviewer

The OIG reviewers are granted read-only access to all program and system-level POA&Ms.

POA&M Coordinator

The POA&M coordinator is responsible for entering updated POA&M and or POA&M data from the System Owners or their designees and consolidating POA&Ms for quarterly submission to the Cyber Security Division (CSD).

Primary Author

The Primary Author is the designated individual with the ability to make updates to all fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping). The Primary Author also has the ability to assign control-level edit access and appendix and narrative update access to him/herself and other users (e.g. Authors, Validators).

Program Manager

The Program Manager is responsible for updating the C&A package with documentation on completed POA&M items (append approved verification form.); and in coordination with the BCISO, the ISO is responsible for providing routine reviews and status reports on corrective actions to the bureau CIO and AO, no less than quarterly.

Senior Agency Information Security Officer

The Senior Agency Information Security Officer or Department Chief Information Security Officer is the DOI official responsible for carrying out the DOI Chief Information Officer IT security and compliance responsibilities under FISMA.

SME - CM

The department has the ability to update the CM report card indicator for each bureau or office.

SME – Incident Response

The department has the ability to update the Incident Response indicators in the report card for each bureau or office.

SME – Training (Department)

The department has the ability to view and update Awareness and IT Professional Training numbers for each bureau or office.

SME – Training (Bureau or Office)

The bureau or office has the ability to update reported training numbers for Awareness and IT Professional Training.

SSP Reviewer

The SSP reviewer is granted read-only view to all SSPs in each assigned bureau or office.

User Representative

User representatives are responsible for the identification of mission/operational requirements and for complying with the security requirements and security controls described in the system security plan. User representatives are individuals that represent the operational interests of the user community and serve as liaisons for that community throughout the life cycle of the information system.

Validator

The Validator is the designated individual with the ability to update only test results, but can be given privilege to update cost, compliance description, and POA&Ms. The Validator can also update narratives and appendices if assigned. The Validator will not be able to update most fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping).

Management Procedures

Bureaus and offices shall comply with the NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, identification and authentication controls identified in the *DOI IT Security Policy Handbook*, Version 3.1, March 18, 2008.

Before an account can be set up in CSAM a User Account Profile worksheet and a System Profile worksheet must be completed. The worksheet format/layout tries to emulate what appears within CSAM.

In the User Account Profile worksheet and the System Profile worksheet DOI has used the comment feature to provide a wealth of additional detailed information. Cells with comments are indicated by a small red triangle in the upper right corner of that cell. Comments are usually immediately available as the document is completed online. Comments can usually be viewed simply by placing the cursor on that particular cell.

AAOs are responsible for all user accounts and systems under their jurisdiction through all phases from creation, annual recertification, and inactivity to retirement. The AAOs (or their duly authorized Representative) must notify their respective AM whenever anyone leaves, transfers, or no longer needs access to CSAM in order to have their account disabled **within two business days** of the event occurring.

Hard copy or fax of input, signatures, etc. is acceptable however not preferred. The preferred media is e-mail; this enables a more efficient method of maintaining a trail of evidence rather than that of paper. Acknowledgements must be explicit. There can be no doubt about who is acknowledging and what they are acknowledging. Please remember that the AM must maintain a trail of evidence for all actions taken. This is especially needed when unusual activities are requested. DOI personnel need to document the authorization as well as the justification for those actions.

User Account

The User Account procedures are provided within the User Account Profile worksheet. CSAM has a means by which the user inputs their personal profile information directly, however, the process to authorize that account, role, and permissions as well as the user's acknowledgement of the DOI Rules of Behavior (ROB) must still be handled manually. A basic CSAM integration evolution within an enterprise involves the establishment of new user accounts.

The worksheet provides procedures to effectively support the profiling of new users so that appropriately profiled new user accounts can be established efficiently and accurately.

The worksheet is divided into three parts:

Part A – User Information. This section identifies general items required such as the user's name, bureau or office name, whether the user is a Government Employee or Contractor and the name of the authorizer of the account (e.g., System Owner) and systems to access.

Part B – Special Access. This section identifies special access privileges for component (also known as bureau or office) users and department/headquarter users. Special access privileges will be granted to bureau/office and department leads only.

Component special access privileges provide:

- * Access to bureau or office Report Card
- * Access to bureau or office FISMA Reports
- * Ability to give existing users access to component SSPs

Department/Headquarter special access privileges provide:

- * Access to Department Programs
- * Access to Department Report Card
- * Access to Department FISMA Reports
- * Ability to give existing users access to SSPs
- * Ability to add SSPs
- * Ability to update Report Card manual columns
- * Ability to run Department POAM Report

Part C - Edit Privileges. This section identifies actions that need to be taken once the information and authorization of Parts A & B have been completed by the user or AAO and inputted by the AM. For example, the name of the system(s) the user should have access to, whether or not the system should be provided during the training phase of the migration process, if the user is to have access to this system for production purposes after migration is complete, if the user should be a/the Primary Author for the System's SSP. [This allows the user to add other users to the SSP and assign them tasks]

The information for Parts A & B must be completed and submitted before the AM can perform the requested action(s). Any and all incomplete forms will be returned to the submitter. The user has limited ability to see their account profile information. Any changes to their account profile information need to be made through the AM. After establishing the CSAM account, the user then needs to be provided access to the systems requested. This can be accomplished by the AM or by a bureau or office lead or Primary Author associated with that system. We prefer that this be accomplished at the bureau or office level so that they are fully engaged with managing their accounts, etc. For a new Primary Author or Author, this is accomplished by going into each system and adding the new user under the "Assign Roles" user access list for that system. A bureau or office lead automatically has access to all systems under that bureau or office. The bureau or office lead should update the "Assign Roles" user access list for each system for documentation purposes.

Part B: Once the system has been established by the actions associated with Part A, at least one user with the Primary Author role should be identified who will be responsible for updating the SSP for this system. The Primary Author will be able to manage user access to this system and add and remove other Authors, and Validators. If they do not already have a user account on the system, a User Profile Sheet must also be submitted by the user's account authorizer.

Incomplete forms may delay the processing of your request(s). Please choose your system names and abbreviations carefully.

Typically this form is used for creating new systems. However, the comments also provide information on retiring systems, adding components, subcomponents and other valuable information.

System Profile Sheet

CSAM c&a Web

CSAM C&A Web System Profile
Please mouse over cells with red triangle in upper right corner for further explanation.

Part A

SYSTEM INFORMATION

System Name	
System Acronym	
Organization	
Sub Organization	
System Scope	
Operational Status	
Contractor System?	
Financial System?	
OMB Reportable?	

Part B

INITIAL USER ACCESS

At least one user with the Primary Author role should be identified here who will be responsible for updating the SSP for this system. The Primary Author will be able to manage user access to this system and add and remove other Primary Authors, Authors, and Validators. If they do not already have a user account on the system, a User Profile Sheet must also be submitted by the user's account authorizer.

Primary Author

Figure 4 System Profile Sheet

The System Profile Sheet is embedded in the following logo. If you double click on the logo, the form will open. It can be saved to a separate file for future use.



Recertification

Recertification of user accounts will be handled directly in CSAM whenever possible, concluding with a report generated from the application that will be sent out for review and signature by the bureau or office AAO (CISO) or CISO designated Representative.

User Account Auditing Procedures

All accounts are automatically locked after 90 days of inactivity. Accounts can also be locked manually by the AM, and a notation can be recorded in a comment field to indicate why the account was locked.

A list of locked accounts is forwarded to the OCIO Client Representative for determination, in conjunction with the bureau or office AO or AM, if the account is still required. If the account is no longer needed, the account status is changed to "Inactive" and the account comments are updated. User capabilities are removed from accounts when they are retired or inactive for more than 90 days and a notation is entered in the account profile. An entry is then made to record when a bureau or office account was audited and the number of accounts locked. OCIO management can then monitor that this weekly audit activity is occurring.

Accounts with user administration capabilities are reviewed on a quarterly basis to determine if user administrator functions are still required.

Definitions

1. **Account**: A logical representation of a user in a system, which allows a user to gain access to the system. Examples of user accounts include the following: Microsoft Active Directory Service accounts, UNIX accounts on individual servers, Oracle database accounts, application accounts, and accounts on devices such as LAN infrastructure equipment.
2. **Account Creation**: The process of creating a new user account.
3. **Account Disablement**: The process of disabling a user account. Disabling a user account does not completely remove the account. Rather, it prevents the user account from being used to gain access to the system.
4. **Account Manager**: A role in the CSAM system that provides ability to activate, edit, and delete user accounts. Also provides ability to assign users to SSPs.
5. **Account Modification**: The process of moving a user from one program office or bureau to another. In such circumstances, an account is moved from one operating system level user group to another.
6. **Account Retirement**: The process of disabling a user account for a user who has departed an organization.
7. **Author**: A role in the CSAM system that will not be able to update most fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping), but can update narratives and appendices that have been assigned. The Author can also update control-level fields (e.g. compliance description, test results, POA&Ms) for those controls that have been assigned.
8. **Control Author**: a role in the CSAM system that is the designated DOI-wide Representative responsible for defining DOI specific controls for developing C&A packages.
9. **Department Lead**: The designated DOI-wide Representative responsible for activating, editing, and deleting bureau and office Account Manager user accounts.
10. **Primary Author**: A role in the CSAM system that has the ability to make updates to all fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping),

can assign control-level edit access and appendix and narrative update access to self and other users (e.g. Authors, Validators).

11. **Transfer Account**: The process of transferring a user account from one office to another office, within the same component.

12. **Validator**: A role in the CSMA system that will not be able to update most fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping). Typically individuals in this role update only test results, but can be given privilege to update cost, compliance description, and POA&Ms. The Validator can also update narratives and appendices if assigned.

Appendix I: CSAM Rules of Behavior

Purpose

The purpose of this document is to explain the Rules of Behavior and requirements to all DOI employees who use CSAM, as specified by OMB Circular A-130, the *DOI IT Security Policy Handbook*, Version 3.1, March 18, 2008, and other related policies. DOI IT resources are the property of the Federal Government and must be protected. Users' access to computing resources indicates a level of trust given to the employees by management and ultimately by DOI. Users must be aware of and acknowledge their actions and their responsibilities when using CSAM in accordance with these Rules of Behavior.

Scope

These Rules of Behavior apply to all employees and contractors who use CSAM. All DOI employees who access CSAM that requires a user ID must be aware of their responsibilities and comply with these Rules of Behavior.

Penalties for Non-Compliance

These Rules of Behavior are founded on the principles described in the DOI published security policies and other regulatory documents such as the Code of Ethics for Government Employees, OPM regulations, OMB regulations, and Standards of Conduct for Federal Employees. Therefore, these rules carry the same responsibility for compliance as the official documents cited above. DOI will apply penalties for noncompliance in a uniform and consistent fashion regardless of race, sex, color, national origin, disability, religion, marital status, grade level, or bargaining unit status of the personnel involved. Account Managers must exercise sound and reasonable judgment in enforcing these Rules of Behavior. Penalties will be assessed in a timely manner. DOI will enforce the use of penalties against any user who willfully violates any DOI or Federal system security policy, including:

- Official, written reprimands,
- Suspension of system privileges,
- Temporary suspension from duty,
- Removal from current position,
- Termination of employment; and
- Possible criminal prosecution.

General Requirements

The Rules of Behavior presented in this document highlight requirements from several laws, policies, and best practices. These Rules of Behavior establish expected and acceptable computing behaviors. Because written guidance cannot cover every contingency, users are also asked to use sound judgment and the highest ethical standards in their decision making.

Access

Users shall access and use only information for which they have official authorization. The following guidelines also apply:

- Follow established procedures for accessing information, including use of user identification, user authentication, passwords, and other physical and logical safeguards,
- Follow established channels for requesting and disseminating information,
- Access only those files, directories, and applications for which access authorization by the system administrator has been granted,
- Use government equipment only for approved purposes,
- Do not give information to other employees or outside individuals who do not have access authority,
- Do not use your trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties; and
- Do not browse files (look to see what you can access).

Accountability

Users are accountable for actions related to information resources entrusted to them.

- Behave in an ethically, technically proficient, informed, and trustworthy manner when using systems,
- Be alert to threats and vulnerabilities such as malicious programs and viruses,
- Prevent others from using your accounts by using procedures such as the following:
 - Log out or lock the screen when leaving the vicinity of your terminal or PC,
 - Set a password on automatic screen savers,
 - Help remedy security breaches, regardless of who is at fault; and
 - Immediately notify the system administrator whenever there is a change in your role, assignment, or employment status and/or when access to the system is no longer required.
- Participate in IT security training and awareness programs,
- Do not install or use unauthorized software on DOI equipment,
- Comply with all software licensing agreements; do not violate Federal copyright laws,
- Practice good citizenship when accessing external systems by complying with that system's rules of behavior; and
- Read and understand banner pages and end user licensing agreements.

Integrity

Users must protect the integrity and quality of information.

- Review quality of information as it is collected, generated, and used to ensure that it is accurate, complete, and up to date,
- Take appropriate training before using CSAM to learn how to correctly enter and change data,
- Protect information against viruses and similar malicious code by:
 - Using virus detection and correction software,
 - Avoiding unofficial software, such as shareware and public domain software; and
 - Discontinuing use of a system at the first sign of virus infection,
- Never enter unauthorized, inaccurate, or false information into a system.

Availability

Computer systems and media must be protected from environmental factors such as fire, water, heat, and food spills. They must also be protected from theft, unauthorized alteration, and careless handling.

- Use physical and logical protective measures to prevent loss of availability of information and systems, such as:
 - Ensuring that there are backups of information for which you are responsible,
 - Protecting systems and media where information is stored,
 - Storing media in protective jackets,
 - Keeping media away from devices that produce magnetic fields (such as phones, radios, and magnets),
- Follow contingency plans; and
- Ensure that more than one individual knows where to find important information and has access rights.

Passwords and User IDs

Users are responsible and accountable for any actions taken under their user ID.

- Protect passwords from access by other individuals,
- Never give a password to another person (including your supervisor or a computer support person); and
- Do not ask anyone for their password.
- Construct effective passwords in accordance with the *DOI IT Security Policy Handbook*, Version 3.1, March 18, 2008.

Privileged Users

Privileged users are those with one or more of the following functions:

- System administrators,
- Departmental CSAM Account Manager,
- System engineers (those with control of the operating system),

- Network administrators;
- Database administrators; and
- Those who control user passwords and access levels.

Privileged users must make an effort to notice the threats to and vulnerabilities of CSAM, call these to the attention of management, and work to develop effective countermeasures.

Privileged users will:

- Respond to security alerts and requests by the Department CISO,
- Protect the supervisor or root-level password at the highest level demanded by the sensitivity of the system,
- Use special access privileges only when they are needed to carry out a specific system function,
- Use a non-privileged account whenever possible,
- Never use special privileges for personal business, gain, or entertainment,
- Use precautionary procedures to protect a privileged account from fraudulent use,
- Establish security measures to ensure integrity, confidentiality, and availability of information contained on the systems,
- Watch for signs of hacker activity or other attempts at unauthorized access,
- Assist with recovery activities and take appropriate action to reduce damage from security violations,
- Alert the appropriate personnel when a system goes down or experiences problems, and
- Ensure that systems and data are properly backed up and that the configuration is adequately documented for recovery purposes.

I acknowledge receipt of the Rules of Behavior; understand my responsibilities, and will comply with the CSAM Rules of Behavior.

Signature

Date

Note: Statement of acknowledgement must be provided to your bureau or office Account Manager.