DHS 4300A

Sensitive Systems Handbook

Attachment H

Process Guide for

Plan of Action and Milestones

(POA&M)

Version 11.0

Fiscal Year 2015

December 3, 2014

Protecting the Information that Secures the Homeland

This page intentionally blank.

Contents

1.0 Introduction 1

1.1 Purpose 1

1.2 Scope Limitation 1

1.3 Applicability 1

1.4 Background 1

1.5 Requirements of Statutes and Policy 2

1.6 Core POA&M Requirements 2

1.7 POA&Ms and Capital Planning and Investment Control (CPIC) 3

2.0 Roles and Responsibilities 4

3.0 DHS POA&M PROCESS 5

3.1 Changes to the POA&M Process with IACS Implementation 6

3.2 Document Weaknesses 8

3.3 Determine Root Cause 8

3.4 Develop a Remediation Strategy 9

3.4.1 Remediation Time Limits 9

3.4.2 Risk Acceptance 9

3.5 Manage to Completion 9

4.0 Financial Systems POA&Ms 9

5.0 POA&M Elements 10

5.1 POA&M Data Elements 10

5.1.1 POA&M Nbr 12

5.1.2 Title 12

5.1.3 Creation Date 12

5.1.4 Weaknesses Description 12

5.1.5 Severity Level 13

5.1.6 Point of Contact 14

5.1.7 Resources Required 14

5.1.8 Scheduled Completion Date 14

5.1.9 Milestones 15

5.1.10 Changes to Milestones 16

5.1.11 Item Identified During (source of weakness) 16

5.1.12 Report ID 17

5.1.13 Overall Status 18

5.1.14 Actual (Completion) Date 19

5.1.15 Comments 19

5.1.16 Approval and Validation 20

5.1.17 DHS CISO Approval 20

5.2 Completing and Closing a POA&M 20

5.2.1 POA&Ms for audit reports 20

5.2.2 POA&Ms for Classified Systems 20

6.0 Weakness Management 20

6.1 Daily Reports 20

6.2 Monthly Reports 21

6.3 IACS Reports 21

6.4 Ad Hoc Reports 21

7.0 POA&M Support 22

Appendix H1 Glossary 23

Appendix H2 Acronyms 26

Appendix H3 Key References 28

Appendix H4 POA&M Process Map 29

Appendix H5 Data Collection 30

Appendix H6 Creation Checklist 33

Appendix H7 Root Cause Analysis 35

Appendix H8 Sample Weakness Descriptions And Milestones 38

Appendix H9 Minimum Resource Estimates 40

Appendix H10 Roles and Responsibilities 49

Appendix H11 Severity Level Determination 52

Appendix H12 CISO/ ISSM Validation Checklist lv

Appendix H13 Document Change History lvi

List of Figures

Figure 1: The main IACS screen, used to initiate a POA&M 11
Figure 2: POA&M Number data element 12
Figure 3: Title field data element 12
Figure 4: Creation Date data element 12
Figure 5: Weakness data element 12
Figure 6: Severity Code data element 13
Figure 7: Point of Contact data element 14
Figure 8: Resources Required data element 14
Figure 9: Scheduled Completion Date data element 15
Figure 10: Waiver Completion Date 15
Figure 11: Milestones data element 15
Figure 12: Changes to Milestones data element 16
Figure 13: Item Identified During data element 17
Figure 14: Report ID Naming Convention data element 17
Figure 15: Report ID default data element 17
Figure 16: Overall Status 18
Figure 17: Actual (Completion) Date data element 19
Figure 18: Comments field data element 19
Figure 19: POA&M Process Map 29
Figure 20: Root Cause Analysis 35

1.0 INTRODUCTION

A Plan of Action and Milestones (POA&M) is mandated by the Federal Information Systems Management Act of 2002 (FISMA) as a corrective action plan for tracking and planning the resolution of information security weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.[1] This Attachment, "Process Guide for Plan of Action and Milestones," to the *DHS 4300A Sensitive Systems Handbook*, constitutes the core process for remediating control deficiencies in sensitive Department of Homeland Security (DHS) information systems.

1.1 Purpose

The purpose of this Attachment is to ensure that the DHS Information Security Program's POA&M process complies with FISMA, with applicable Office of Management and Budget (OMB) directives, and with DHS Management Directives.

The guidance in this Attachment is written to assist DHS and its Components in implementing the POA&M process. The purpose of the process is to assist in documenting, prioritizing, remediating, and monitoring corrective actions. Correcting deficiencies is an integral part of management accountability and is considered a priority at DHS.

1.2 Scope Limitation

This POA&M Process Guide is not intended to be an Information Assurance Compliance System (IACS) user manual; the manual is available online at: https://iacs.dhs.gov/xacta.

1.3 Applicability

This process applies to all Department and Component programs and information systems where information security weaknesses have been identified. Within the context of this guide, "system" refers to any Major Application (MA), General Support System (GSS), or other system listed in the DHS FISMA system inventory. Any individual tasked with completing POA&M activities should read and apply this process to achieve FISMA compliance.

1.4 Background

In its Memorandums titled "Reporting Instructions for the Federal Information Security Management Act," OMB annually issues guidance that further details the goals of the POA&M process, its required elements, and performance expectations. An extensive list of references is contained in Appendix H3 of this Attachment.

[1] OMB Memorandum 02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," October 17, 2001.

1.5 Requirements of Statutes and Policy

DHS Sensitive Systems Policy Directive 4300A, Section 1.1 states that policy elements are effective when issued, and non-implementation of a policy element within ninety (90) days of publication shall be considered a weakness; requiring that the Component generate either a system or program POA&M. Whenever IACS requires updating to reflect policy element changes, tool changes shall be available to the Department within forty-five (45) days of the policy changes.

The **Federal Information Security Management Act (FISMA)** requires that every Federal department and agency develop and implement a POA&M process to document and remediate information security weaknesses and to periodically report progress to OMB and to Congress.

OMB Publications contain requirements issued by the Office of Management and Budget (OMB), which is the implementation and enforcement arm for Presidential policy. OMB requires departments and agencies to prepare POA&Ms for all programs and systems, where an information security weakness has been found. Additionally, OMB requires program officials to regularly update the Chief Information Officer (CIO) on the progress of POA&Ms so that the CIO can monitor remediation efforts and provide quarterly updates to OMB. Updates should occur at least quarterly, and may be directed ad-hoc by the CIO. Therefore, it is important that the POA&M data managed by each Component be kept current in the DHS IACS tool.

1.6 Core POA&M Requirements

The term *POA&M* refers to an authoritative *plan of action and milestones* for correcting an information system security weakness. OMB Memorandum 04-25 states that a POA&M is a tool that identifies tasks that need to be accomplished. A POA&M should contain a detailed estimate of the resources required to accomplish the elements of the plan, milestones to be passed in accomplishing the task, and scheduled dates for reaching each milestone.

OMB intends that a POA&M:

- Be a management tool to help identify and track remediation of identified weaknesses
- Assist agencies in closing their security performance gaps
- Assist the Office of Inspector General (OIG) in evaluating agency security performance
- Assist OMB with discharging its oversight responsibilities

POA&Ms provide a high level view of what needs to be done to correct information technology (IT) weaknesses. The weaknesses may be combined, summarized or paraphrased in the POA&M for ease of management understanding, but the original source, such as test results from IT control audits or assessments that identified the weakness, should be available. Each POA&M should be clearly traceable back to its original source(s).

In some cases, additional, more detailed project management plans may be needed for each corrective action item identified in the POA&M; however, resolution of each weakness must proceed according to a POA&M.

1.7 POA&Ms and Capital Planning and Investment Control (CPIC)

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

The CPIC administrator list and reference information is found on the Enterprise Business Management Office (EBMO) site through DHS Connect.

2.0 ROLES AND RESPONSIBILITIES

Each Component must ensure that the required POA&M responsibilities are being accomplished.

Management is responsible for ensuring that the required controls are designed properly and operating as intended. As part of this responsibility, management sets the entity's objectives, implements controls, and evaluates the internal control system. However, personnel throughout an organization play important roles in implementing and operating an effective internal control system. The recommended POA&M responsibilities for each of the following roles are fully detailed in Appendix H10:

- DHS Chief Information Security Officer (CISO): As Risk Executive, establishes the standards for system security risk, oversees risk management and monitoring, approves all waivers to *DHS Sensitive Systems Policy Directive 4300A.*
- Component CISOs: As Risk Executives, oversee and monitor the progress of POA&M implementation and remediation efforts of their Component.
- Authorizing Official (AO): Has inherent U.S. Government authority and is assigned to Government personnel only; approves plans of action and milestones and is accountable for the security risks associated with information system operations with the level of authority commensurate with understanding and accepting such information system-related security risks.
- System Owners: Are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security.
- Security Control Assessor (SCA): Must be a Federal employee and must be free from any perceived or actual conflicts of interest; the SCA certifies the results of the security control assessment.
- Component Information Systems Security Managers (ISSM): Monitor progress of POA&M implementation efforts.
- Common Control Provider: Ensures that POA&Ms are developed for all common controls having weaknesses or deficiencies.
- Component Information Systems Security Officers (ISSO): Develop, track, and manage POA&Ms for systems under their control.
- Program Managers: Provide copies of program POA&Ms to the affected System Owner; responsible for program-level POA&Ms that may impact one or more systems.

3.0 DHS POA&M PROCESS

The DHS POA&M process begins with developing a remediation plan, which should be completed by the scheduled completion date. A POA&M Process Map is provided in Appendix H4. The process includes:

- Determining the root cause of the vulnerability or IT weakness with stakeholder involvement, including estimating the resource cost to complete the corrective actions and who should be involved in resolving the weakness
- Determining the severity level of the weakness in order to prioritize POA&M efforts according to risk factors
- Developing a timeline for remediation by defining activities that should be clearly identifiable, easily measurable, and have an achievable completion date
- Assigning responsibility for remediation, and developing internal controls to monitor and update the POA&M to demonstrate weekly to monthly progress
- Monitoring IT weaknesses to prevent delays in scheduled completion dates
- Well planned, executed, and monitored POA&Ms should be able to achieve passing scores on the monthly weakness remediation metric.

3.1 Changes to the POA&M Process with IACS Implementation

POA&M creation and management processes have been modified to support the change in several data elements due to the implementation of IACS, which replaces Trusted Agent FISMA (TAF). The table that follows is a crosswalk showing the data element name changes and the data elements that are no longer present.

POA&M Data Elements		IACS – Process Notes	
TAF	**IACS**	**Functional Status (✓= functionality present)**	**Comments**
Class	No replacement	Removed	The specific class designations have been removed from the security control families by NIST SP 800-53, Rev 4.
Family	No label	✓	No label appears, but the deficient security control can be entered and it appears in the weakness field if test matrix is used
Weakness Number	POA&M Nbr:	✓	No change; generated by system
Creation Date	Creation Date (mm/dd/yyyy)	✓	No change; the current date is automatically inserted
Finding	No replacement	✓	The Comments section should be used to document the finding
Weakness Description	Weakness	✓	No change
Status	Overall Status	✓	*Expired* is the system generated change in status that occurs when the scheduled completion date is not met
Criticality (Priority)	No label	Changed	Merged into Severity Code
Point of Contact (POC)	Point of Contact	✓	Not auto-populated based on log-in
Risk Category	No label	Changed	Merged into Severity Code
Resources Required	Resources Required	✓	Same data is required
Severity	Severity Code	Changed	The severity level is risk based: High Moderate Low
Type	No label	Changed	Defined through the “Project” naming convention
Scheduled Completion Date	Scheduled Completion Date (mm/dd/yyyy)	✓	No calendar icon; the date format is the same
Is Material Weakness	No replacement	Removed	Removed

POA&M Data Elements		IACS – Process Notes	
TAF	**IACS**	**Functional Status (✓= functionality present)**	**Comments**
Estimated Completion Date	No replacement	Removed	Removed
Exclude from OMB Reporting	No replacement	Removed	Removed
Actual Completion Date	Actual Date (mm/dd/yyyy)	✓	No calendar icon; the date format is the same
Risk Accepted	No replacement	Removed	Removed from POA&M creation
Link to Control Title	No label	✓	Appears in the weakness description; auto-populated when test matrix is used
Weakness ID	No replacement	Removed	Removed
Identified In	Item Identified During:	✓	Slight name change, but functionally is the same
Report ID	Report ID:	✓	Rules of use and naming convention are the same
ISSM Validation	No label	Changed	Appendix C of Performance Plan; required as an internal control for each Component to manage
HQ Review	No label	Changed	Appendix C of Performance Plan; DHS CISO Approval Check; internal control review for headquarters
Milestone Description	Milestones:	✓	No change
Milestone Scheduled Completion Date	Scheduled Completion Date	✓	A date field has been added to capture the scheduled completion dates of milestones.
Milestone Actual Completion Date	Actual Completion Date	✓	A date field has been added to capture the scheduled completion dates of milestones.
	Waiver Expiration Date	New	A date field has been added to capture and track the expiration dates of waivers.

3.2 Document Weaknesses

As it applies to POA&Ms, the term *weakness* means an information security vulnerability that could be exploited by a threat source to compromise the confidentiality, integrity, or availability of an information system, system security procedure, internal control, or other security implementation.

Weaknesses are usually identified during a formal review process. At DHS, a POA&M must be developed for every weakness identified during any of the following:

- Audits (OIG, Government Accountability Office (GAO), FISMA, Financial System)
- OMB A-123 Internal Control Review
- Independent Verification and Validation (IV&V)
- Security Assessment Report (SAR)
- Security Control Assessment (SCA)
- Common Control Catalog Authorization or Validation (For information systems inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation is also included in the authorization package. *NIST -800-37*, Task 5-2)
- Critical Control Review (CCR)
- Program Review
- Vulnerability Assessments
- IT Acquisition Review (ITAR) process
- Other sources that may reveal a weakness. For example, if a security incident reveals that a system has no process for applying patches, a POA&M should be created to document the Corrective Action Plan (CAP) for creating such a process.

3.3 Determine Root Cause

Determining the root cause of a weakness is essential to ensuring that the "true" cause of the weakness, and not its symptom(s), is properly addressed. An organization's policy, procedures, or people are generally the underlying root cause(s) of any weakness.

Appendix H7, "Root Cause Analysis," provides guidance and steps to follow when performing the analysis.

3.4 Develop a Remediation Strategy

The remediation strategy should be the result of collaborative stakeholder efforts. The stakeholders include the program officials, business process owners, system owners, CISOs, ISSMs, ISSOs, system administrators, and others within the scope of remediation. After weaknesses have been identified and the root cause has been determined, a plan must be developed.

3.4.1 Remediation Time Limits

- Remediation of system-level weaknesses must be accomplished within six months or less.
- For program-level issues, such as those that are enterprise-wide, the maximum time for remediation is five (5) years.

3.4.2 Risk Acceptance

Non-compliance with any element of DHS Sensitive Systems Policy Directive 4300A requires corrective action to achieve compliance. The DHS CISO has the authority to extend the remediation time with a waiver on a case-by-case basis when deemed justified. The DHS Sensitive Systems Handbook, Section 1.5 provides guidance on the waiver process.

3.5 Manage to Completion

POA&M data should be monitored on a continuing basis and updated as events occur. Refer to Appendix H12 for the *CISO/CISO Designated Alternate/ISSM Validation Checklist.*

As part of their review, CISOs/ISSMs should:

- Validate that the weakness is properly identified and prioritized;.
- Ensure that appropriate resources have been made available to resolve the weakness; and.
- Ensure that the schedule for resolving the weakness is both appropriate and achievable.

4.0 FINANCIAL SYSTEMS POA&MS

DHS Components are required to develop a POA&M for each recommendation contained in the Information Technology Notice of Finding and Recommendation (IT NFR) issued to them. The POA&M must include milestones for testing both the design and operating effectiveness of the control.

Two milestones that are required in every POA&M are:

- Testing the design of a control to determine whether the control exists and is designed properly to achieve its objective
- Testing the operating effectiveness of a control to determine whether the control is operating effectively as intended

POA&Ms for IT NFRs must be completed within thirty (30) days after the IT NFR is signed by DHS Management.

5.0 POA&M ELEMENTS

Components must use IACS to identify, track, and manage all IT system weaknesses and associated POA&Ms to closure for Sensitive But Unclassified (SBU) systems. Users who need access to IACS may request an account and appropriate privileges through their CISO or ISSM. Help Desk Support for IACS is available by telephone at 202-343-2500 or via email at isosupport@hq.dhs.gov.

Detailed instructions for using IACS are provided in an on-line user's guide available by clicking the "Technical Support" link at the bottom of the IACS homepage and selecting the "Training materials" tab. A number of other useful reference documents and training materials are available through the IACS portal, which is available on the Intranet at http://mgmt-ocio-sp.dhs.gov/ciso/compliance/iacs.

Classified-Trusted Agent FISMA (C-IACS), still in operation and being used for recording POA&Ms and other data for classified systems, is available through the Homeland Secure Data Network (HSDN). Help Desk Support for C-TAF is available via telephone at 202-343-2500 or via email at isosupport@hq.dhs.gov.

5.1 POA&M Data Elements

The following sections describe data that must be captured in a POA&M to meet OMB and DHS requirements. A worksheet for collecting POA&M data is located in Appendix H5. The main IACS screen used to build a POA&M item is shown below.

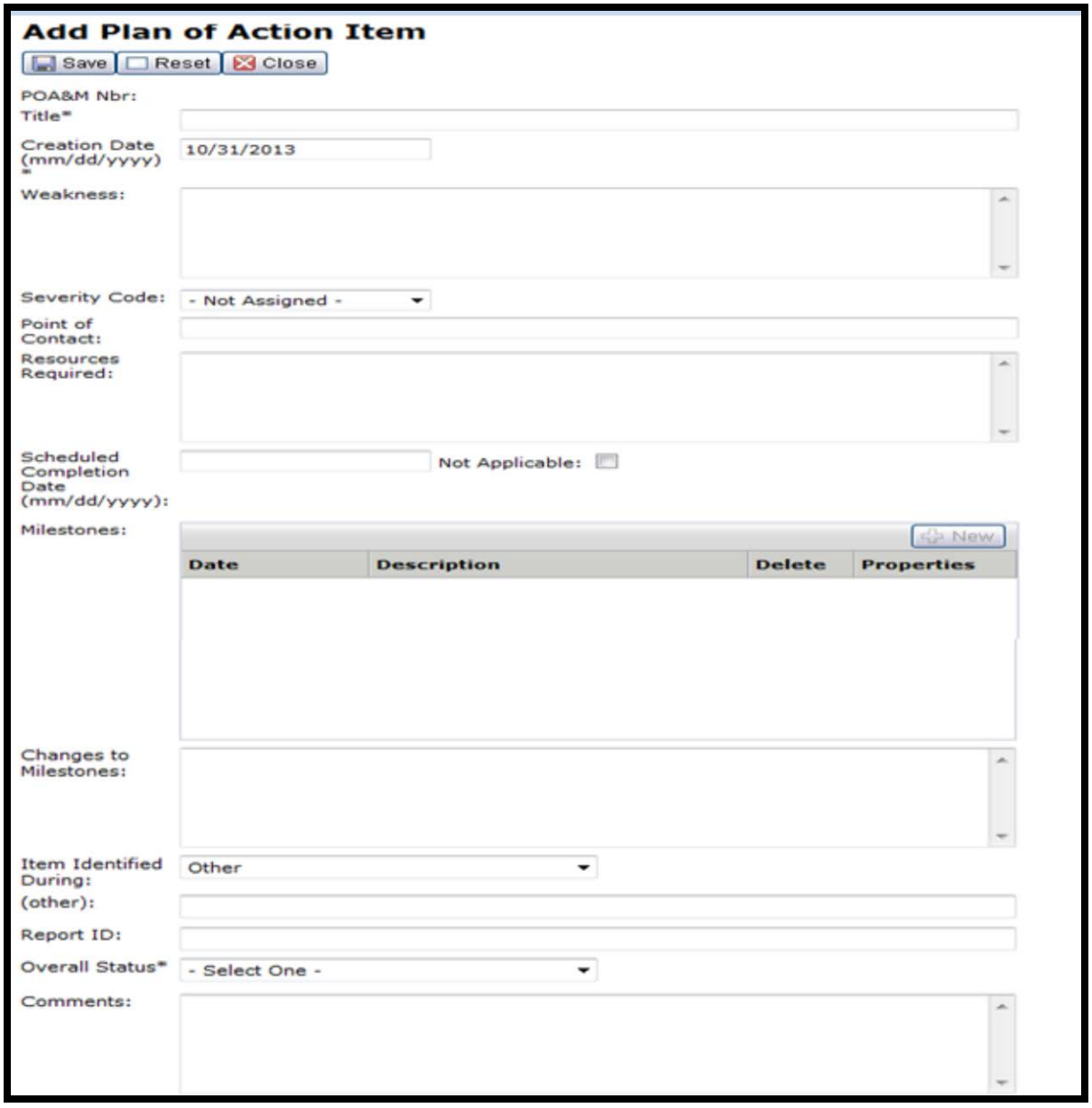

Figure 1: The main IACS screen, used to initiate a POA&M

5.1.1 POA&M Nbr

The POA&M number is a unique sequential number for each weakness that is automatically assigned by IACS.

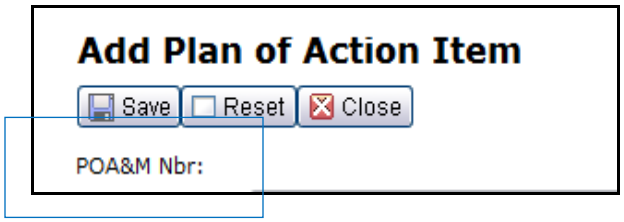

Figure 2: POA&M Number data element

5.1.2 Title

The weakness number (POA&M number) also appears in the TITLE field. ***This logic will be revisited with the vendor.***

Figure 3: Title field data element

5.1.3 Creation Date

The creation date is the start date for the corrective actions and must be filled in by the user upon POA&M creation. Per OMB requirements, the creation date cannot be changed after the POA&M is saved.

Figure 4: Creation Date data element

5.1.4 Weaknesses Description

All NIST 800-53 controls that have not been satisfied in controls testing, as well as a description of the weakness, should be entered in the "Weakness" field. The weakness description should not simply repeat the control statement from NIST 800-53, nor should it be a cut and paste of the recommendation from an audit report.

Figure 5: Weakness data element

5.1.5 Severity Level

The severity level should be selected from the "Severity Code" field list box (opened by clicking on the down arrowhead). Descriptions of each level are given below. The severity code values can be set to I, II, III, and IV or Low, Moderate, and High respectively.

Figure 6: Severity Code data element

- I – Significant Deficiency: 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.
- II – Reportable Condition: A security weakness not deemed to be a significant deficiency by agency management, yet affecting the efficiency and effectiveness of agency operations.
- III - Other Weakness: This option should be selected unless guided by your Component's Risk Executive.
- IV - Not Assigned: The POA&M will fail the Information Security scorecard POA&M metric if this option is selected.

Guidance on risk-based decision making for POA&Ms is found in NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems." that :

Organizations should define a strategy for developing POA&Ms that facilitates a prioritized approach to risk mitigation consistent across the organization. The strategy helps to ensure that organizational POA&Ms are based on:

- The security categorization of the information system.
- The specific weaknesses or deficiencies in the security controls.
- The importance of the identified security control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the overall security state of the information system, and hence on the risk exposure of the organization, or ability of the organization to perform its mission or business functions). This is the organization's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions and allocation of risk mitigation resources). A risk assessment guides the prioritization process for items included in the POA&Ms.

Refer to **Appendix H11** for additional guidance on determining severity level.

5.1.6 Point of Contact

A Point of Contact (POC) must be listed for each POA&M weakness. The POC should be someone who is knowledgeable about the program or system and about the weakness. The name, title, and contact information for the POC (i.e., telephone number and email address) should all be entered in the "Point of Contact" field.

Figure 7: Point of Contact data element

5.1.7 Resources Required

The resources required and source of the funding that will be used to remediate each identified weakness must be entered into the "Resources Required" field. The resources required must be entered as a dollar amount. Appendix H provides estimated resource amounts for remediating various types of NIST 800-53 control weaknesses; but the POA&M is expected to augment the minimum provided to include the additional costs of remediating the weakness specific to the Component environment. Estimates should include the costs of labor for government and contractor employees, hardware, software, licenses, training, travel, and support and maintenance fees as applicable.

Ensure that the funding source is identified as:

- **Funded in current budget** means that the required activities are already ongoing or are planned and funded; no action is needed to obtain additional resources. For example, a new firewall will be installed and tested by existing staff.
- **Reallocation of base resources** means that resources planned for a different purpose will be used to remediate this weakness. For example, plans to upgrade servers have been postponed and the funds to obtain the servers will now be used to procure a firewall.
- **Request for new funding anticipated** means that there are currently no resources available to remediate the weakness and new funding will be needed. Anytime the "Request for new funding anticipated" option is selected, a milestone must be included to show the actions needed to obtain the funding.

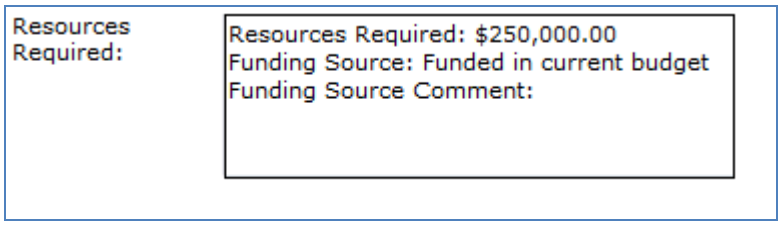

Figure 8: Resources Required data element

5.1.8 Scheduled Completion Date

Non-completion date should be based on a realistic estimate of the amount of time it will take to perform a root cause analysis, to plan corrective action, to allocate the needed resources, and to complete the corrective action. It is important to assign a scheduled completion date that is reasonable, because once the date is entered and the POA&M is approved, the date cannot be

changed. Reviewers will accept only final versions of POA&M documents, so it is important to factor in sufficient time for review and testing into the timeline.

System POA&Ms that cannot be completed within six (6) months, as required by the DHS Information Security Performance Plan, require a waiver for non-compliance with DHS policy. Refer to *DHS Sensitive Systems Handbook 4300A,* Attachment B, for guidance on waivers and the required request form.

The scheduled completion date for resolving the entire weakness should be entered in the "Scheduled Completion Date" field in IACS.

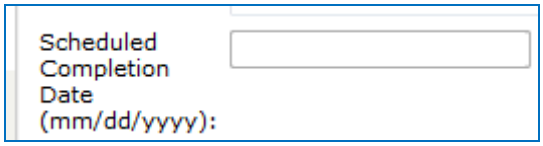

Figure 9: Scheduled Completion Date data element

Figure 10: Waiver Completion Date

5.1.9 Milestones

Milestones should effectively communicate the major steps that will be performed to remediate the weakness. The number of milestones should reflect the number of major steps or corrective actions necessary to address the weakness. At a minimum, the POA&M should include one milestone for every quarter the POA&M is open.

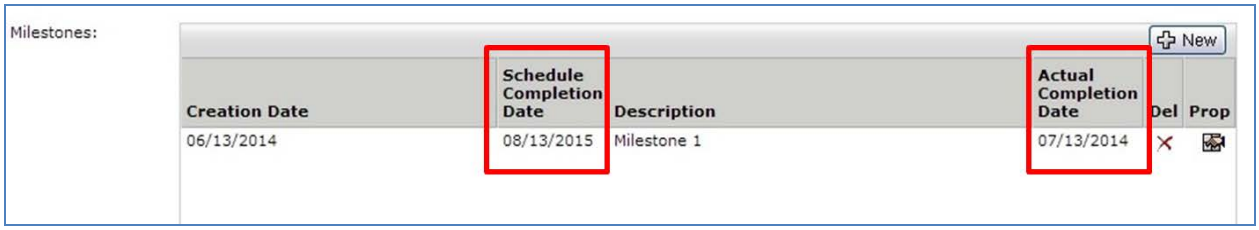

Figure 11: Milestones data element

A POA&M should include testing the design of the control, as well as testing whether the control is operating effectively after the corrective actions have been completed. To ensure that these key steps are not omitted, the POA&M should include the following two milestones.

- Test the design of the control to determine that it has been properly developed or established to accomplish the required task.

- Test the effectiveness of the control to verify that it actually performs as intended by design.

A milestone to test whether the control is operating effectively should be the last step performed with a positive result before changing the status of the POA&M to complete.

Milestones should not simply repeat a description of the weakness, but should rather describe an action needed to correct the weakness. For example, appropriate milestones for a weakness like, "patches are not current" could include:

- Determine root causes
- Update patch policy
- Develop procedures to standardize the patch update process;
- Establish a test environment for implementing patches before applying them to the production environment
- Test the process
- Update system patches

Appendix H8 contains additional guidance and examples of acceptable and unacceptable milestone descriptions.

Section 4.0 describes the milestones required for financial systems.

5.1.10 Changes to Milestones

If there are changes to any of the milestones or their scheduled completion dates that do not affect the overall completion date, they should be entered in the Changes to Milestones field. Changes cannot be made to the original estimate in either the "Scheduled Completion Date" or the "Milestones with Completion Date" data element fields.

Figure 12: Changes to Milestones data element

5.1.11 Item Identified During (source of weakness)

Every weakness identified must be captured in a POA&M. Each POA&M must have at least one weakness source identified using the drop down menu in the "Item Identified During" data element field. If the source is not listed, select other.

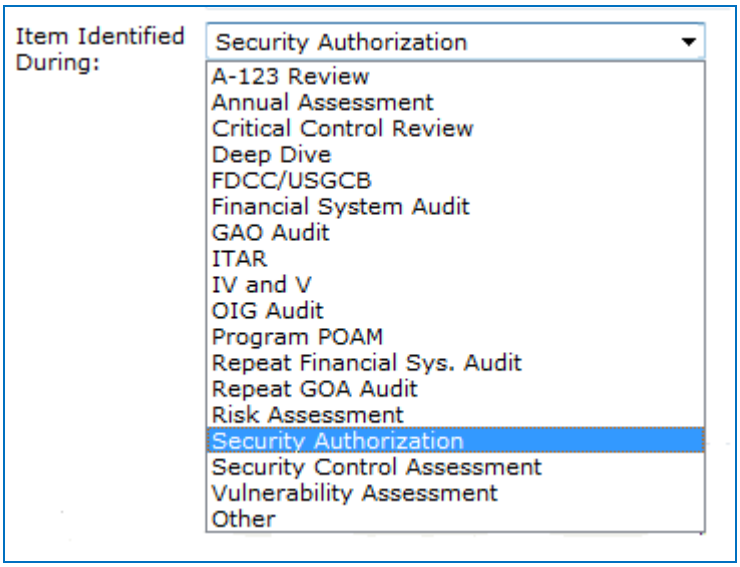

Figure 13: Item Identified During data element

The goal is to ensure that all weaknesses are addressed and that a POA&M is created to resolve every identified weakness. New sources can be added to open POA&Ms.

5.1.12 Report ID

In the Report ID data element, the following naming conventions are required for the sources listed:

- OIG audits – OIG-2 digit fiscal year-OIG assigned report number (e.g., OIG-11-017)
- GAO audits – GAO-2 digit fiscal year-GAO assigned report number (e.g., GAO-11-44)
- IT Notice of Findings and Recommendations (IT NFR)- the naming convention for the IT NFR would be the IT NFR number (e.g., OCISO-IT-11-17)
- OMB A-123 ITGC Assessment –Component-A123-fiscal year-recommendation number (e.g., ICE-A123-11-25)

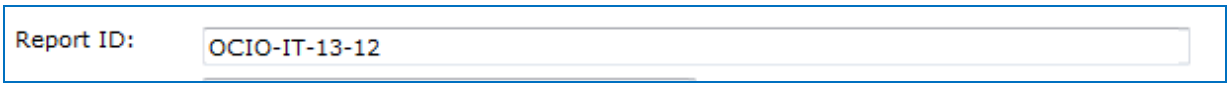

Figure 14: Report ID Naming Convention data element

When a Report ID is not entered, the data element auto populates with the default data of NONE-0.

Figure 15: Report ID default data element

5.1.13 Overall Status

Each weakness must be assigned a status, and the POA&M must be maintained to indicate the current status of corrective action progress. The status is one of six allowed by IACS and assigned using the list box in the "Overall Status" data element field.

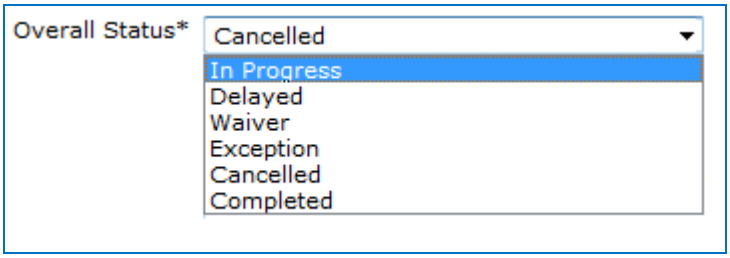

Figure 16: Overall Status

In Progress should be used once any activities to resolve a weakness have begun. Such activities may include planning (for example, creating a POA&M), procurement actions, coordination activities, or actual remediation actions. This category is the default in IACS and can be used properly in any case except completed, cancelled, waivered, or delayed. Note that there is no official distinction between *In Progress*, *Ongoing*, *Not Started*, and *Planned Pending*. *In Progress* is the preferred entry for all new POA&Ms, but Components may use any of the other entries for internal tracking purposes.

Waiver should be considered when a POA&M will take longer than six (6) months to complete and the delay is justifiable. When this status is used, a DHS CISO-approved DHS waiver form must be uploaded in IACS. Use of this status category must be approved in IACS by the Component CISO. The Component Chief Financial Officer (CFO) must approve waiver requests for CFO-designated systems prior to the submission of such waiver requests to the DHS CISO.

Any waiver request for Privacy Sensitive Systems must be submitted to and approved by the Component's Privacy Officer or senior Privacy Point of Contact (PPOC) prior to being submitted to the DHS CISO. Any waiver for compliance with privacy controls must be submitted to and approved by the DHS Chief Privacy Officer.

Waiver requests must follow procedures in the DHS Sensitive Systems Policy Directive 4300A, using the guidance published in the *DHS 4300A Sensitive Systems Handbook*, Attachment B.

Completed should be used only when a weakness has been remediated and the corrective action has been tested and approved. Corrective action testing should therefore be incorporated into the weakness mitigation process and identified as a milestone.

Cancelled may be used when the condition that was identified as a weakness has changed although the weakness has not been remediated. Examples of justification for a status of Cancelled include:

- The risk has been accepted by the AO after the weakness has been entered in the POA&M
- The affected system is retired
- The responsibility for a system has been transferred to another Component

The reason for cancellation of the POA&M must be selected from the dropdown menu in IACS. When "Other" is selected as a reason, an explanation must be entered in the box provided. A POA&M with a status of "Cancelled" requires approval from the Component CISO in IACS.

Delayed should be used if corrective action for a weakness will be completed after the Scheduled Completion Date. IACS automatically changes the status to "Delayed" when the Scheduled Completion Date has passed. Use of this status category must be approved by the Component CISO in IACS. When the status is delayed, a new estimated completion date must be entered in the appropriate field in IACS (see Section 6.2.16) and a reason for the delay must be selected from the dropdown menu in IACS after clicking. Examples of reasons for delay include:

- Weakness priority changed
- Original completion time underestimated
- Funds not allocated, or insufficient funding
- Assigned funds reallocated
- Dependency on other task(s)
- Contractor delay
- Procurement delay
- Personnel shortage
- Technical dependency
- Other (describe in notes)

5.1.14 Actual (Completion) Date

Once a weakness is resolved and all milestones are completed, the actual completion date should be entered in the *Actual Date* field. When the actual completion date is entered, the "Overall Status" should also be changed to "Completed."

Figure 17: Actual (Completion) Date data element

5.1.15 Comments

The *Comments* data element is an open text area and is available for use as a notes section for information sharing about the progress of the Corrective actions, including issues.

Figure 18: Comments field data element

5.1.16 Approval and Validation

As part of their oversight responsibilities, Component CISOs or designated alternates are required to monitor the status of POA&Ms. Prior to approving a POA&M for closure, the Component CISO or designee should review the artifact(s) uploaded as evidence that the corrective actions have been completed and the control is operating effectively for adequacy. CISOs must also formally approve all POA&Ms with a status of "Delayed", "Cancelled", "Waiver" or "Exception." As of DHS Sensitive Systems Policy Directive 4300A version 11.0, exceptions are no longer granted; the choice will be eliminated from future versions of IACS software.

5.1.17 DHS CISO Approval

This field is completed by DHS HQ only. DHS CISO approval is a manual review. A key area of review is the milestone descriptions, to determine if they are written as action items to remediate the weakness, as incremental steps and dates to accomplish remediation, or as professional judgment about the likelihood of completion or repeat status.

5.2 Completing and Closing a POA&M

When all milestones have been completed, the POA&M may be closed. To close a POA&M, select the status "Completed" from the dropdown list box and change the "Actual Completion Date" field to contain the date the final action was completed.

5.2.1 POA&Ms for audit reports

POA&Ms for audit reports that are issued as repeat findings with a new audit or IT NFR number should not be closed, even if the prior year finding is closed by the auditor. As long as the original finding remains unresolved, the original POA&M should remain open and additional or repeat findings should be added to the Report ID.

5.2.2 POA&Ms for Classified Systems

Each National Security System **must** have a POA&M to document the plan for resolving its weaknesses. POA&Ms for classified systems should be developed and entered in C-IACS following the procedure given in Section 4 of this document. No classified data should ever be entered into the unclassified version of IACS.

6.0 WEAKNESS MANAGEMENT

DHS produces a variety of daily, monthly, and quarterly reports to track the status of POA&M activity. These reports are described below.

6.1 Daily Reports

Via Crystal Reports, DHS produces a daily report listing POA&Ms that do not meet performance plan standards. The report is automatically available to CISOs and ISSMs and to a select group of designated users at each Component. Requests for distribution of this report should be made to the Component CISO or ISSM. Details on elements that are included in the scorecard and grading criteria can be found in the current year DHS Information Security Performance Plan.

6.2 Monthly Reports

DHS produces a monthly scorecard which includes metrics on POA&M quality, management, completeness, reasonableness, and closure timeliness. There are two scorecard metrics designed to help the DHS Office of the Chief Information Security Officer (OCISO) to monitor POA&M progress, identify potential problem areas and provide feedback to Department and Component managers. It is disseminated to the CISO Council and to the CIO Council. Details on the included elements and on grading criteria can be found in the current year DHS Information Security Performance Plan.

6.3 IACS Reports

The IACS tool has been enhanced with an Executive Dashboard reporting capability, which is a suite of executive reports that can be customized and retained by the user. Please refer to the reports section of IACS for user guidance.

6.4 Ad Hoc Reports

IACS users may also request special reports through the DHS InfoSec Customer Service Center at DHSInfosecHelpdesk@hq.dhs.gov or IsoSupport@hq.dhs.gov. These special reports provide information from IACS that cannot be produced by the user through self-generated "stock" or "canned" reports. Ad Hoc reports can be saved and sent to the user as requested.

In addition to summary sheets, each Component also receives a number of feeder reports which describe with detailed data the elements that contribute to each section of the scorecard.

7.0 POA&M SUPPORT

POA&M support is available from several sources. The DHS Information Security Help Desk is an excellent source for answers to questions about both IACS and the POA&M process and may be reached at 202-343-2500 or via email at ISOSupport@hq.dhs.gov. POA&M Subject Matter Experts (SME) are available by phone through the helpdesk to answer questions or provide "how to" help. Additionally, Review and Assist Visits are available if requested. These visits are tailored to meet the specific requirements of the requesting organization and can range from formal training sessions for Information Systems Security Officers (ISSO) or others through a one-on-one hands-on practicum using the Component's system data.

APPENDIX H1 GLOSSARY

Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the NIST Publications, OMB Circulars, and GAO auditing resources.

Capital Planning and Investment Control (CPIC): "…a decision-making process for ensuring that investments integrate strategic planning, budgeting, procurement, and the management of in support of Agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues." [OMB Circular A-11]

Common Control: A security control that is inherited by one or more organizational information systems. *See Security Control Inheritance.* [CNSSI 4009, April 2010]

Control Deficiency: Control deficiencies exist when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A design deficiency exists when a control necessary to meet the control objective is missing or an existing control is not properly designed, so that even if the control operates as designed the control objective is not always met. An operation deficiency exists when a properly designed control does not operate as designed or when the person performing the control is not qualified or properly skilled to perform the control effectively. [Office of Management and Budget (OMB) Circular A-123, "Management's Responsibility for Internal Control," December 21, 2004]

Corrective Action Plan (CAP): The plan formulated to document the procedures and milestones identified to correct control deficiencies.

Deficiency: A weakness in the design, implementation, or operation of a control that could management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks.

Evidence: any information used by the auditor, tester, or evaluator, to determine whether the information being audited, evaluated, or assessed is stated in accordance with the established criteria.

Exhibit 53: also referred to as agency IT investment portfolios. Required by OMB Circular A-11 and provide summary budget information for all agency major and non-major IT investments. [OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," July, 2014.

Exhibit 300 Business Case: Exhibit 300 business cases are also referred to as capital asset plans. They are required by OMB Circular A-11 and provide budget justification and reporting requirements for investments. They provide agencies with the format to report on the budgeting, acquisition, and management of federal capital assets.

Information System Security Officer (ISSO): Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. [CNSSI 4009]

Internal Control: Internal control, in the broadest sense, includes the plan of organization, methods and procedures adopted by management to meet its goals. Internal control includes processes for planning, organizing, directing, controlling, and reporting on agency operations.

The three objectives of internal control are:

1. Effectiveness and efficiency of operations,
2. Reliability of financial reporting, and
3. Compliance with applicable laws and regulations

[OMB Circular A-123, based on U.S. Government Accountability Office (GAO) "*Standards for Internal Control in the Federal Government*," November 1999, commonly called the "Green Book."

Material Weakness: A deficiency in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. [Accounting Institute definition]

A material weakness exists when one or more Material weaknesses under FMFIA include reportable conditions which the Secretary or Component Head determines to be significant enough to report outside of the Department. A material weakness in internal control over financial reporting is a reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.

Metrics: Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. [NIST Interagency or Internal Reports (NISTIR) 7298 Rev 2 "Glossary of Key Information Security Terms," May 2013]

Plan of Action and Milestones (POA&M): A FISMA mandated corrective action plan to identify and resolve information security weaknesses. A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

[OMB Memorandum 02-01]

Program: An organized set of activities directed toward a goal or particular set of goals or objectives for which the program is accountable; a distinct set of activities and strategies organized toward achieving a specific purpose. In government, a program is a representation of what is delivered to the public. Programs usually operate for indefinite or continuous periods, but may consist of several projects or initiatives. [DHS Management Directive 1330, "Planning, Programming, Budgeting and Execution," February 14, 2005]

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [CNSSI 4009]

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical

structures, areas, and devices; synonymous with security controls and countermeasures. U.S. GAO, "Federal Information System Controls Audit Manual (FISCAM)," February 2, 2009

Security Control Inheritance: A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. NIST SP 800-53, which appends to the definition [See also *Common Control*]

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSSI 4009]

The undesirable impact can come in many forms, but often results in a financial loss. A threat agent could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates that security policy, a tornado wiping out a facility, or an employee making an unintentional mistake that could expose confidential information or destroy a file's integrity.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [CNSSI 4009]

Weakness: The absence of adequate controls. [See also *Deficiency*]

APPENDIX H2 ACRONYMS

Acronym	Meaning
AO	Authorizing Official
BLSR	Baseline Security Requirements
CAP	Corrective Action Plan
CCR	Critical Control Review
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
C-IACS	Classified Information Assurance Compliance System
FIPS	Federal Information Processing Standard
DHS	Department of Homeland Security
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers Financial Integrity Act
GAO	Government Accountability Office
GSS	General Support System
HSDN	Homeland Secure Data Network
IACS	Information Assurance Compliance System
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITAR	IT Acquisition Review
IT NFRS	Information Technology Notice of Findings and Recommendations
IV&V	Independent Verification and Validation
MA	Major Application
MD	Management Directive
NIST	National Institute of Standards and Technology
OIG	(DHS) Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
POC	Point of Contact

Acronym	Meaning
SAR	Security Assessment Report
SCA	Security Control Assessor
SP	Special Publication
TAF	Trusted Agent FISMA
UII	Unique Investment Identifier

APPENDIX H3 KEY REFERENCES

Federal Laws

Federal Information Security Management Act of 2002 (FISMA), 44 USC 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899

OMB Circulars

Office of Management and Budget Circular A-130, "Management of Federal Information Resources," revised, November 30, 2000

OMB Memorandums

Two OMB Memorandums provide key guidance for what is required of agency POA&Ms:

M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," October 17, 2001; and

M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004

These documents can be found at http://www.whitehouse.gov/omb/memoranda/index.html.

Department of Homeland Security Publications

DHS Management Directive MD 140-01, "Information Technology Systems Security," July 31, 2007

[Note: DHS MD 4300-1, previously a reference for this attachment, was superseded by MD 140-01.]

DHS Sensitive Systems Policy Directive 4300A, v11.0, April 30, 2014

DHS 4300A Sensitive Systems Handbook, v9.1, June 2012

"DHS Information Security Performance Plan, Fiscal Year 2012," April 30, 2012. Performance Plan links are found on the DHS Intranet at http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/comtech.aspx

NIST Federal Information Processing Standards (FIPS)

National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

NIST Information Technology Security Special Publications (SP)

National Institute of Standards and Technology (NIST) Special Publications (SP) 800 Series, especially NIST SP 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April, 2013. Current NIST SPs are found at http://csrc.nist.gov/publications/PubsSPs.html

APPENDIX H4 POA&M PROCESS MAP

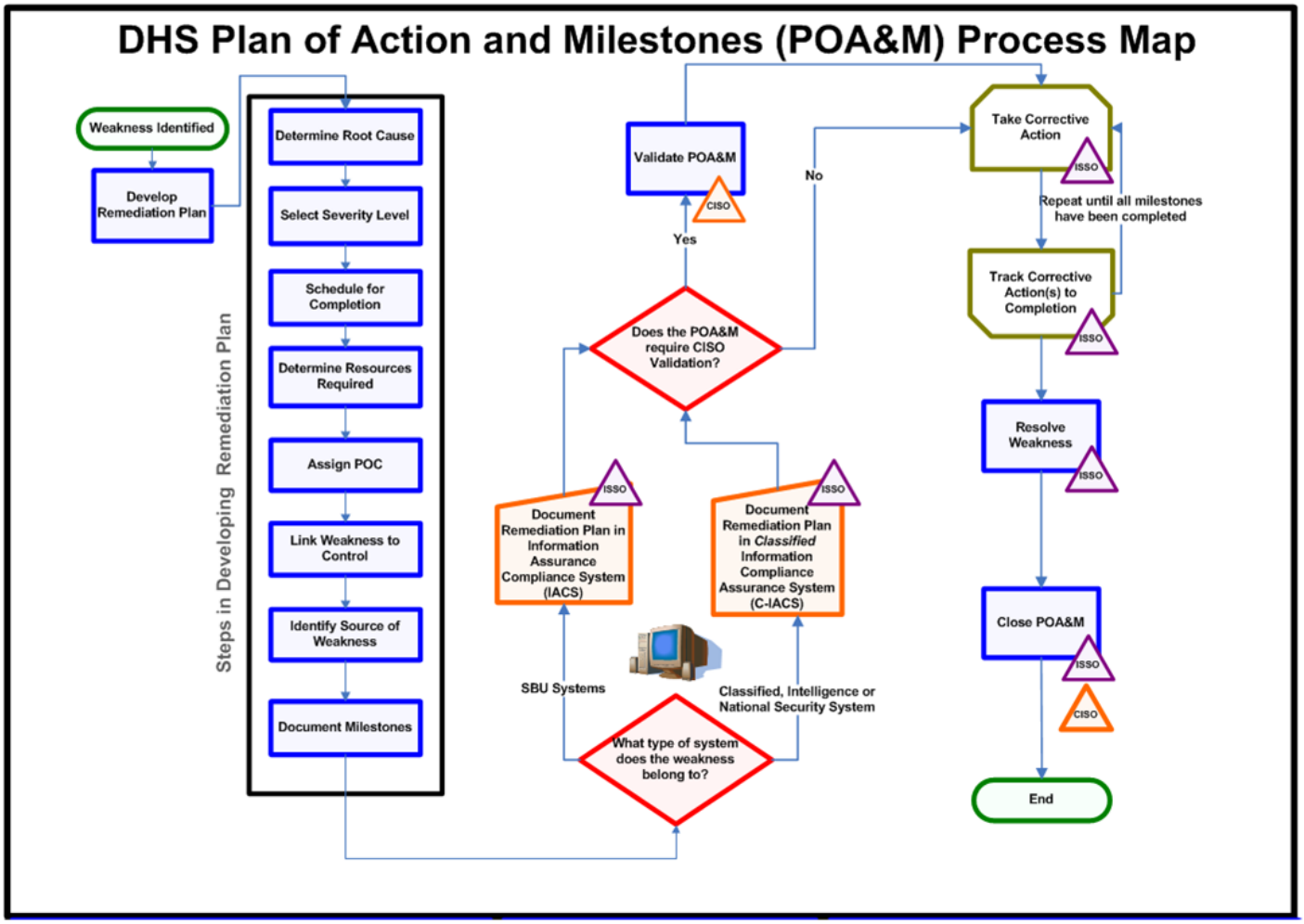

Figure 19: POA&M Process Map

APPENDIX H5 DATA COLLECTION

The following worksheet should be used in unison with the POA&M Creation Checklist (Appendix H6). The suggested use of the worksheet is as a planning tool to collect the data for a POA&M before it is entered into IACS. Most of the information entered into the IACS tool is locked down once it is saved. The worksheet assists in ensuring that the POA&M is ready to be created with the fewest changes possible. Although milestone changes are expected, creation date changes are not.

Point of Contact (POC)

Who will be responsible for ensuring this weakness is remediated (i.e., POC)?

Name _____

Phone _____

E-mail _____

Who will be responsible for resolving this weakness? _____

Who are the stakeholders that should be involved in planning and implementation activities? What is their preferred mode of notification?

_____

_____

Weakness Source (*Item Identified During* field in IACS)

What is the source of the weakness?

_____

Audit report number (refer to section 5.0) _____

IT NFR number (refer to section 5.0) _____

Was this weakness previously identified by another source? If so, document each source.

_____

_____

Resources

Who will do the work? How many hours will it take? What is their hourly rate?

_____

_____

What other resources are needed (hardware, software, licenses, training, etc.)? Are they available or will they have to be purchased?

_____

_____

_____

Where will resources come from?

( ) Are resources available? (Funded in current budget)

( ) Will resources be diverted from another area? (Reallocation of base resources)

( ) Will new funding be requested? (Request for new funding anticipated)

Weakness/Control Deficiency (See Appendix H8, Reasonableness Criteria)

What is the NIST SP 800-53 control that is failing?

- Locate the control on the Reasonableness Criteria for entry as a minimum cost for resources
- If multiple controls are failing, add them together as a minimum data point for resources

_____

What is the weakness/control deficiency?

_____

_____

Root Cause

What is the root cause of the weakness (see Appendix H7, "Root Cause Analysis")?

_____

_____ _____

Milestones

What activities/steps are needed to resolve the weakness?

- Identify steps needed to resolve the weakness

  _____

  _____

  _____

- Testing/validation activities

  _____

  _____

Schedule Completion Date (milestones)

When will each of the steps needed to resolve the weakness be completed? Do not enter the same date for each milestone; it is unrealistic for each milestone to be completed on the same date.

_____

_____

Is this schedule realistic and achievable? Are there any steps that could be delayed by circumstances beyond your control?

_____

_____

Schedule Completion Date (overall POA&M) - What is the internal tracking and monitoring approach to stay on top of the progress made toward completion?

_____

NOTE: Full remediation and timely completion are the goals of each deficiency being remediated.

APPENDIX H6 CREATION CHECKLIST

The following checklist should be used in unison with the POA&M Data Collection worksheet located in Appendix H4, while referring to Sections 4 and 6 of this guide along with Appendix C of the Information Security Performance Plan.

This POA&M creation checklist is intended to walk the user through the "Add Plan of Action Item", which is the POA&M creation screen in IACS, to help ensure all fields are filled in properly. This activity assumes that data has already been assembled, properly coordinated with stakeholders, and that the user has a basic understanding of the information required.

Creating a POA&M

POA&Ms for IT security control deficiencies found during IT audits on financial systems, annual FISMA compliance testing, and other internal and external reviews are created outside of the IACS tool's Security Authorization workflow. The following guidance on creation of a POA&M assumes creation outside of the Security Authorization workflow.

Within the "Folders & Project" section of IACS, click on the relevant Project (information system or program) this will take you to "Tasks", scroll to "Monitor POA&M," click on POA&M Elements, then at the menu bar, click on "NEW" to bring up the "ADD PLAN OF ACTION ITEM" screen.

- The **POA&M Number** is automatically filled in by IACS, ***after*** save has occurred. (A modification request is in the works to change this sequence of events).
- **Title** is automatically filled in by IACS and restates the POA&M number as follows:
- The **Creation Date** defaults to today's date.
- The **Weakness** data element in IACS also requires that the NIST 800-53 control is entered at the beginning before the weakness description is entered. Enter the appropriate description of the weakness in the Weakness field – This text cannot be changed after saving, so ensure accuracy prior to saving.
- Select the **Severity** from the drop down. Other weakness is preferred unless a risk-based management decision provides specific instruction on severity level.
- Enter required **Point Of Contact** data
- The **Status** field defaults to **In Progress**
- Enter **Resource** amount in whole dollars
- Enter the **Scheduled Completion Date** – cannot be changed. The date must be realistic and achievable, but less than 6 months distant for a system POA&M and less than 5 years distant for a program POA&M.
- Enter the **Milestone** information, which should consist of actions to remediate the vulnerability/weakness/finding/recommendation. The dates should not be the same for

each milestone. It is unrealistic that each corrective action noted in the milestone would be completed on the same day. Milestone dates should show progression toward remediation.

- A **change to Milestone is** one of the few edits allowed to be made by IACS users. As the plan of action progresses, adjust the milestone activity as needed.
- **Item Identified During** is the statement of how the vulnerability/weakness/finding/ recommendation was discovered. The drop down menu provides the most common options. If the source is not listed in the drop down, select other, but a selection must be made.
- **Report ID** uniquely identifies the IT Audit source of the finding or recommendation and is reserved for tracking those weaknesses and ensuring they are captured as POA&Ms.
- **Overall Status** defaults to In Progress.
- **Comments** section is an open text box that can be used to communicate internal notes for Component unique communication about the remediation activities.
- The **Actual Completion Date** is blank and only used when the POA&M is completed.

Completing a POA&M

To Complete a POA&M:

- All **Milestones** must be complete.
- Artifacts to support status must be uploaded.
- Internal testing is required to validate complete status.
- Once testing validates status and artifacts support status, Component CISO or delegated alternate approval is required.
- Component CISO or delegated alternate should change the status to **Complete**.
- Component CISO or delegated alternate should enter the **Actual Completion Date**.
- **Save** the POA&M.
- Select **Save** and select **Close**.

APPENDIX H7 ROOT CAUSE ANALYSIS

Root cause analysis is a structured systems analysis methodology whose purpose is to identify the underlying causes of problems, issues, and/or events. The goal of root cause analysis is to identify the underlying problem(s) and solution(s) to problems by attempting to bound, correct, or eliminate underlying causes, as opposed to merely addressing the immediately obvious symptoms. This is important because correcting the underlying root cause may eliminate more than one seemingly unrelated symptom or address a prevalent issue across an entire organization.

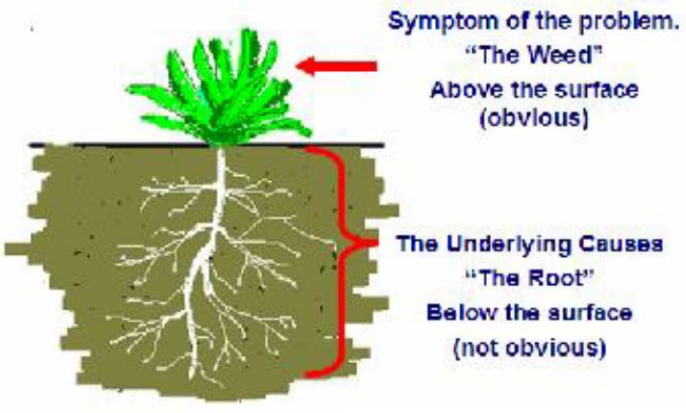

Figure 20: Root Cause Analysis

Reasons for conducting a root cause analysis include:

- To help system owners and stakeholders understand information security impact to mission and operations
- To assist system owners, CISO and Information Systems Security Officers (ISSO) with the assignment of risk and subsequent prioritization for remediation
- To identify underlying causes for control weaknesses in order to strengthen issues which are preventing the control from working as designed and/or implemented.
- To document root causes provide broader understanding of control gaps
- To reduce the likelihood of control recurrence by focusing corrective actions on the cause versus the systematic conditions which are more frequently reported.

There is usually more than one root cause for any given problem. It follows that a root cause can be reflected by more than one symptom. To be most effective, the analysis should address all known causal relationships between the root cause(s) and the identified problem(s). When performing root cause analysis, always consider **Policies, Procedures, Process, People, and Systems Technology and Resources** in the investigation. For example, technical symptoms often have procedural or people-oriented root causes, a poorly implemented internal control for example. Root cause analysis should be performed in an iterative manner, each iteration building upon the work of the previous one, and brain storming by a group of people with divergent backgrounds and expertise should be encouraged to develop the most robust solutions.

Root cause analysis worksheets are provided at the end of this section to help the analyst identify, categorize, and document the root cause of a security control weakness or vulnerability. The form may also be used to assist in documenting the root cause of a weakness identified from multiple types of sources (*e.g.*, audit, security authorization, ST&E, annual assessment, etc.)

At a minimum, the following steps are recommended when conducting a root cause analysis:

- **Understand the impact of the identified problem** (i.e., a security control weakness) on business or mission needs; do not focus on the symptoms or technology issues. Try to first understand the problem, the context for the problem, and the stakeholders of the problem. Do not start investigating possible solutions until the problem is bound and defined from the people, process, and technology perspectives; otherwise the solution may bias the root cause analysis.
- **Consider the known threats and vulnerabilities** associated with the security control weakness and understand the risk to and impact on the organization, the location, the program or project, the system, and the data and information.
- **Work with the system owners, CISO, ISSM, ISSOs, and audit liaisons** to help prioritize the order in which control weaknesses should be addressed. For example, is the control weakness identified as a material weakness? Is it a significant deficiency or a reportable condition? Does it impact more than one Component system or site?
- **Identify and walk through** the following potential root causes associated with the security control weakness:
- **Review the applicable Policies** to determine if they provide clear requirements. Determine if the DHS guidance (e.g., DHS MD 4300A Sensitive System Policy or Handbook as well as Component Policy or Handbooks) are being appropriately and consistently applied. Contact the policy staff at your Component or DHS headquarters if clarifications are needed.
- **Review the latest applicable control Procedures** (e.g., as referenced in NIST SP 800-53) to determine if the procedures are understood, and the expected control design and implementation is documented in the System Security Plan (SSP). Evaluate and document if the control is considered a critical "key control". Review the underlying security requirement (independent of the solution) and consider functional control requirements for quantity, quality, coverage, timelines, and availability.
- **Review existing Business Processes or Standard Operating Procedures (SOP)**. Consider business process descriptions and compensating controls. Are they part of the documented security control design and implementation requirements?
- **Review the Systems Technology**, including security architecture and security services being used to implement and support the control. Determine whether the hardware platform, Operating System and application software are adequate to meet the internal control design and implementation requirements.
- **Identify the People** who are responsible for developing, implementing, documenting, testing and continuously monitoring the security control (*e.g.*, ISSO, system administrators, supervisors, etc.) Determine if they are aware of and understand the

procedures they are responsible for supporting. Has the staff been sufficiently trained and do they follow the procedures?

- **Identify the Resources** needed to properly implement and monitor the internal control (for example people, hardware, software licenses, software development time, implementation, test, documentation, training, and continual monitoring of effectiveness, etc.). Is the solution achievable with current resources (staff, funding, and systems) within the next 6 to 12 months or does the system owner and/or other principal stakeholder (*e.g.*, Component CIO, CFO) want to consider a waiver or exemption request? Is the remediation / mitigation activity (i.e., the solution) cost justifiable? Root cause analysis should determine if current resources can address the control weakness or if additional longer range funding for resources will need to be requested (*e.g.*, OMB Exhibit 300 funding requests, etc.).

Common Root Causes

Each control weakness will generally be a unique combination of factors. The following is a partial list of some examples of root causes:

- Lack of current, written policy and/or procedures.
- Component policies are inaccurate or otherwise inadequate
- Standard Operating Procedures are not being followed, i.e. Emergency Fixes applied without record of change management approvals.
- Is notification of critical security patches being received by the Operations Staff and is implementation ensured by tracking?
- People (Staff)
- Poor or inconsistent communication between the System Owner, ISSO, and System Administrators, System Operator.
- Assigned ISSO supporting higher priority collateral duties.
- The operational staff is not properly trained to performing control functions (e.g. which alerts are critical for identification when reviewing Security Log Files).
- Systems Technology
- The hardware platform has reached end of life and is no longer being upgraded and only basic hardware maintenance activities are supported.
- Does the operating system include configuration management for hardening? Do insecure services or default accounts need to be removed?
- Control cannot be implemented on the current platform, i.e. only weak passwords are supported.
- Security Log Files not turned on or being overwritten.

APPENDIX H8 SAMPLE WEAKNESS DESCRIPTIONS AND MILESTONES

This Appendix provides examples of weakness descriptions and milestones to illustrate what is considered compliant with OMB and DHS guidance and what is not. Examples of non-complaint weaknesses and milestones provide a rationale regarding why they are non-compliant with suggestions for improving them. Accurately defining the weakness is the first step toward developing a good remediation plan.

Compliant Sample Weakness Descriptions

Below are examples of actual weaknesses extracted from IACS that illustrate descriptions that are compliant with DHS and OMB guidance. They are stated as weaknesses that need to be resolved and identify the core issue. They can easily be mapped to a control title.

- Privileged accounts are not secured by authentication technology stronger than that based only on a UserID and password.
- Terminated and/or separated user accounts are not removed on a timely basis.
- Backup tapes are stored in the same building as the production server.
- There are not adequate procedures for documenting and correcting vulnerabilities found in quarterly vulnerability scans.
- No ISA exists.
- Application does not initiate a session lock after a period of inactivity.
- Password protected screen savers are not set to activate within 5 minutes of inactivity.
- Inadequate system documentation.
- Humidity controls are not deployed in the server rooms that house servers. Humidity levels are not consistently maintained / monitored in the server rooms. No redundant systems are available in the event of an outage of the temperature control systems.

Milestone Examples

Below are sample milestones extracted directly from IACS that properly capture the actions that are needed to resolve the weakness.

- Update CPT documentation to reflect DHS comments listed in CPT Checklist.
- Set all passwords to expire per DHS policy
- Turn off Telnet and implement SSH on all switches

The following table, extracted from, IACS, are examples of actual milestones that illustrate a series of steps to address and resolve a particular weakness. They include steps for planning, testing, implementing and documenting the proposed solution.

Investigate options for verifying supervisor approval of Form 20-24
Select most suitable option and update procedures.
Implement ongoing process for re-certifying system users.
Test effectiveness of new process by cross checking form 20-24 against active user list.

Develop SOPs to define and assign specific roles and responsibilities for managing accounts on the system
Define a process to disable accounts after a person has left DHS or a DHS component.
Hand over control of the system from Engineering to Operations Team. Provide formal document or email with handoff signature.
Define password expiration and verify that this setting is in place for this system. System. Accounts should lock out or expire after a defined period of inactivity.
Assure that DHS password guidelines are being followed for complexity on this system. Provide a screenshot of this setting.
Submit a system change request to the technical review committee to set failed login threshold
Set login threshold and analyze any negative effects that may occur from new configuration
Test logon threshold within TDL.
Deploy threshold to production environment
Document in detail the process for performing system backups in accordance with DHS policy.
Document the frequency, process, location, etc. of the backup process
Back up information and store in a secure location.
Verify backup media reliability and information integrity on a regular scheduled basis.
Ensure that there are daily backup tapes in the alternate location, or that the tapes in at the primary site are stored in a secure location, separate from the data center.

APPENDIX H9 MINIMUM RESOURCE ESTIMATES

The POA&M reasonableness metric for FY15 includes a check for remediation costs (i.e. resources). This metric was prepared to address OIG FISMA recommendations that DHS check POA&Ms for reasonableness. The metric is included under the POA&M Quality metric. Like other quality metrics, POA&M reasonableness will be scored on a pass / fail basis at the system level (aggregating the POA&Ms under a system).

The POA&M reasonableness criteria are not intended to replace the planning process as described in the DHS POA&M Process Guide. Nor is it intended to provide an expected cost. Rather, it is designed as a check to ensure that ISSOs do not enter data that does not meet the estimated minimum to remediate the specified control.

The resource estimates provided below have been developed to address a range of data that is considered to be the minimum resources "reasonable" for remediating the specified control. **They are not intended as nor should they be used as a guideline for what it should cost to correct a weakness.**

The resource estimates provided represent the minimum level of effort (LOE) required to resolve a weakness. Resource estimates are based on a nominal labor rate of $100 per hour and do not include other direct expenses (e.g., hardware or software). Because of the wide range of potential circumstances affecting any specific control, the "best possible case" was used to determine LOE. Below are rules of thumb used in computing LOE.

- Documents (policies, procedures, etc.): minimum of 4 hours or $400 to complete.
- Configuration hardening weaknesses: a minimum of ½ hour or $50. In some cases, only one part of a control may not be implemented.
- Resources needed to prepare security authorization documentation were based on estimated times given in the Certification and Accreditation Guidance for SBU Systems User's Manual, Appendix B.
- Weaknesses where a cost could not be estimated due to the complexity of the task or unknown factors (e.g., installing a fire suppression system) have been consistently listed at a nominal $50.

800-53 Control	Control Name	Minimum Resources
AC-1	• Access Control Policy And Procedures	≥ $400
AC-2	• Account Management	≥ $50
AC-3	• Access Enforcement	≥ $50
AC-4	• Information Flow Enforcement	≥ $200
AC-5	• Separation of Duties	≥ $200
AC-6	• Least Privilege	≥ $250
AC-7	• Unsuccessful Login Attempts	≥ $50
AC-8	• System Use Notification	≥ $50
AC-9	• Previous Logon (Access) Notification	≥ $50
AC-10	• Concurrent Session Control	≥ $50
AC-11	• Session Lock	≥ $50
AC-12	• Session Termination (Withdrawn)	≥ $50
AC-13	• Supervision and Review—Access Control (Withdrawn)	≥ $400
AC-14	• Actions Permitted Without Identification or Authentication	≥ $200
AC-15	• Automated Marking (Withdrawn)	≥ $50
AC-16	• Security Attributes	≥ $50

800-53 Control	Control Name	Minimum Resources
AC-17	• Remote Access	≥ $2000
AC-18	Wireless Access	≥ $2000
AC-19	Access Control for Mobile Devices	≥ $4000
AC-20	Use of External Information Systems	≥ $400
AC-21	User-Based Collaboration and Information sharing	≥ $400
AC-22	Publicly Accessible Content	≥ $400
AT-1	Security Awareness and Training Policy and Procedures	≥ $400
AT-2	Security Awareness	≥ $2000
AT-3	Security Training	≥ $4000
AT-4	Security Training Records	≥ $4000
AT-5	Contacts with Security Groups and Associations	≥ $400
AU-1	Audit and Accountability Policy and Procedures	≥ $400
AU-2	Auditable Events	≥ $400
AU-3	Content of Audit Records	≥ $400
AU-4	Audit Storage Capacity	≥ $400
AU-5	Response to Audit Processing Failures	≥ $800
AU-6	Audit Review, Analysis, and Reporting	≥ $400
AU-7	Audit Reduction and Report Generation	> $1000
AU-8	Time Stamps	> $50
AU-9	Protection of Audit Information	> $50
AU-10	Non-Repudiation	> $50
AU-11	Audit Record Retention	> $400
AU-12	Audit Generation	> $100
AU-13	Monitoring for Information Disclosure	> $100
AU-14	Session Audit	> $100
CA-1	Security Assessment and Authorization Policies and Procedures	> $400

800-53 Control	Control Name	Minimum Resources
CA-2	Security Assessments	> $5000
CA-3	Information System Connections	> $2000
CA-4	Security Certification (Withdrawn)	> $92000
CA-5	Plan of Action and Milestones	> $1800
CA-6	Security Authorization	> $500
CA-7	Continuous Monitoring	> $100
CM-1	Configuration Management Policy and Procedures	> $400
CM-2	Baseline Configuration	> $4000
CM-3	Configuration Change Control	> $4000
CM-4	Security Impact Analysis	> $2400
CM-5	Access Restrictions for Change	≥ $50
CM-6	Configuration Settings	≥ $50
CM-7	Least Functionality	≥ $50
CM-8	Information System Component Inventory	≥ $400
CM-9	Configuration Management Plan	≥ $100
CP-1	Contingency Planning Policy and Procedures	≥ $400
CP-2	Contingency Plan	≥ $5200
CP-3	Contingency Training	≥ $2500
CP-4	Contingency Plan Testing and Exercises	≥ $10000
CP-5	Contingency Plan Update (Withdrawn)	≥ $1200
CP-6	Alternate Storage Sites	≥ $4000
CP-7	Alternate Processing Sites	≥ $4000
CP-8	Telecommunications Services	≥ $4000
CP-9	Information System Backup	≥ $200
CP-10	Information System Recovery and Reconstitution	≥ $400
IA-1	Identification and Authentication Policy and Procedures	≥ $400
IA-2	Identification and Authentication (Organizational Users)	≥ $50

800-53 Control	Control Name	Minimum Resources
IA-3	Device Identification and Authentication	≥ $50
IA-4	Identifier Management	≥ $400
IA-5	Authenticator Management	≥ $50
IA-6	Authenticator Feedback	≥ $400
IA-7	Cryptographic Module Authentication	≥ $100
IA-8	Identification and Authentication (Non-Organizational Users)	≥ $400
IR-1	Incident Response Policy and Procedures	≥ $400
IR-2	Incident Response Training	≥ $400
IR-3	Incident Response Testing and Exercises	≥ $1200
IR-4	Incident Handling	≥ $1200
IR-5	Incident Monitoring	≥ $400
IR-6	Incident Reporting	≥ $400
IR-7	Incident Response Assistance	≥ $100
IR-8	Incident Response Plan	≥ $400
MA-1	System Maintenance Policy and Procedures	≥ $400
MA-2	Controlled Maintenance	≥ $800
MA-3	Maintenance Tools	≥ $400
MA-4	Non-Local Maintenance	≥ $400
MA-5	Maintenance Personnel	≥ $50
MA-6	Timely Maintenance	≥ $2000
MP-1	Media Protection Policy and Procedures	≥ $400
MP-2	Media Access	≥ $400
MP-3	Media Marking	≥ $400
MP-4	Media Storage	≥ $400
MP-5	Media Transport	≥ $400
MP-6	Media Sanitization	≥ $400

800-53 Control	Control Name	Minimum Resources
PE-1	Physical and Environmental Protection Policy and Procedures	≥ $400
PE-2	Physical Access Authorizations	≥ $50
PE-3	Physical Access Control	≥ $50
PE-4	Access Control for Transmission Medium	≥ $50
PE-5	Access Control for Output Devices	≥ $50
PE-6	Monitoring Physical Access	≥ $800
PE-7	Visitor Control	≥ $400
PE-8	Access Records	≥ $400
PE-9	Power Equipment and Power Cabling	≥ $100
PE-10	Emergency Shutoff	≥ $50
PE-11	Emergency Power	≥ $50
PE-12	Emergency Lighting	≥ $50
PE-13	Fire Protection	≥ $50
PE-14	Temperature and Humidity Controls	≥ $50
PE-15	Water Damage Protection	≥ $50
PE-16	Delivery and Removal	≥ $400
PE-17	Alternate Work Site	≥ $50
PE-18	Location of Information System Components	≥ $1000
PE-19	Information Leakage	≥ $1000
PL-1	Security Planning Policy and Procedures	≥ $400
PL-2	System Security Plan	≥ $4000
PL-3	System Security Plan Update (withdrawn)	≥ $2000
PL-4	Rules of Behavior	≥ $400
PL-5	Privacy Impact Assessment	≥ $200
PL-6	Security-Related Activity Planning	≥ $50
PS-1	Personnel Security Policy and Procedures	≥ $400

800-53 Control	Control Name	Minimum Resources
PS-2	Position Categorization	≥ $50
PS-3	Personnel Screening	≥ $50
PS-4	Personnel Termination	≥ $50
PS-5	Personnel Transfer	≥ $50
PS-6	Access Agreements	≥ $50
PS-7	Third-Party Personnel Security	≥ $400
PS-8	Personnel Sanctions	≥ $50
RA-1	Risk Assessment Policy and Procedures	≥ $400
RA-2	Security Categorization	≥ $200
RA-3	Risk Assessment	≥ $4000
RA-4	Risk Assessment Update (Withdrawn)	≥ $2000
RA-5	Vulnerability Scanning	≥ $400
SA-1	System and Services Acquisition Policy and Procedures	≥ $400
SA-2	Allocation of Resources	≥ $400
SA-3	Life Cycle Support	≥ $400
SA-4	Acquisitions	≥ $400
SA-5	Information System Documentation	≥ $400
SA-6	Software Usage Restrictions	≥ $50
SA-7	User Installed Software	≥ $400
SA-8	Security Engineering Principles	≥ $400
SA-9	External Information System Services	≥ $400
SA-10	Developer Configuration Management	≥ $400
SA-11	Developer Security Testing	≥ $4000
SA-12	Supply Chain Protection	≥ $400
SA-13	Trustworthiness	≥ $400
SA-14	Critical Information System Components	≥ $400

800-53 Control	Control Name	Minimum Resources
SC-1	System and Communications Protection Policy and Procedures	≥ $400
SC-2	Application Partitioning	≥ $50
SC-3	Security Function Isolation	≥ $50
SC-4	Information in Shared Resources	≥ $50
SC-5	Denial of Service Protection	≥ $50
SC-6	Resource Priority	≥ $ 50
SC-7	Boundary Protection	≥ $50
SC-8	Transmission Integrity	≥ $100
SC-9	Transmission Confidentiality	≥ $100
SC-10	Network Disconnect	≥ $50
SC-11	Trusted Path	≥ $50
SC-12	Cryptographic Key Establishment And Management	≥ $50
SC-13	Use of Cryptography	≥ $50
SC-14	Public Access Protections	≥ $50
SC-15	Collaborative Computing Devices	≥ $50
SC-16	Transmission of Security Attributes	≥ $50
SC-17	Public Key Infrastructure Certificates	≥ $400
SC-18	Mobile Code	≥ $400
SC-19	Voice Over Internet Protocol	≥ $400
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	≥ $100
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	≥ $100
SC-22	Architecture and Provisioning for Name/Address Resolution Service	≥ $100
SC-23	Session Authenticity	≥ $100
SC-24	Fail in Known State	≥ $50
SC-25	Thin Nodes	≥ $50

800-53 Control	Control Name	Minimum Resources
SC-26	Honeypots	≥ $50
SC-27	Operating System-Independent Applications	≥ $50
SC-28	Protection of Information at Rest	≥ $50
SC-29	Heterogeneity	≥ $50
SC-30	Virtualization Techniques	≥ $50
SC-31	Covert Channel Analysis	≥ $50
SC-31	Information System Partitioning	≥ $50
SC-33	Transmission Preparation Integrity	≥ $50
SC-34	Non-Modifiable Executable Programs	≥ $50
SI-1	System and Information Integrity Policy and Procedures	≥ $400
SI-2	Flaw Remediation	≥ $50
SI-3	Malicious Code Protection	≥ $50
SI-4	Information System Monitoring	≥ $50
SI-5	Security Alerts, Advisories, and Directives	≥ $50
SI-6	Security Functionality Verification	≥ $50
SI-7	Software and Information Integrity	≥ $50
SI-8	Spam Protection	≥ $50
SI-9	Information Input Restrictions	≥ $50
SI-10	Information Input Validation	≥ $50
SI-11	Error Handling	≥ $50
SI-12	Information Output Handling and Retention	≥ $50
SI-13	Predictable Failure Prevention	≥ $50

APPENDIX H10 ROLES AND RESPONSIBILITIES

Role	Responsibility
DHS Chief Information Security Officer (CISO) or their designated DHS Risk Executive	Develops information security policy, establishes the standards for system security risk, oversees risk management and monitoring, and approves all waivers and exceptions to DHS policy Oversee and maintain the DHS POA&M process. Provides an enterprise POA&M process for IT security weaknesses. Ensures that the POA&M process prioritizes corrective actions for information security weaknesses. Ensure that information security weaknesses are addressed in a timely manner. Conducts independent reviews of POA&M quality Submits quarterly FISMA reports to OMB to include required POA&M data. Allocates resources necessary to permit identification and remediation of the Information Security Office (ISO) program and system weaknesses. Allocates proper resources to support Department-wide POA&M process implementation and reporting mechanisms.
Component Chief Information Officers (CIOs) / Component Risk Executive	Implements the system security risk management and monitoring program and submitted requests for higher-risk deviations from the enterprise standard. May establish standards for system security risk more stringent than the DHS standard. Ensures that corrective action plans for all programs and systems are developed, implemented, and managed. Reports the results of Component system and program reviews and progress in implementing the POA&M. Allocates proper resources to permit identification and remediation of weaknesses. Oversees and monitors progress of POA&M implementation and remediation efforts for their Component.

Role	Responsibility
Component CISOs / Component Risk Executive /Component ISSMs	May establish standards for system security risk more stringent than the DHS standard. Works with Program Officials, Systems Owners, and ISSOs to build and implement a comprehensive POA&M process at the Component level. Monitors progress of Component POA&M implementation efforts. Approves the priority level each time the status of a priority level 4 o4 5 POAM changes in IACS. This includes the POA&M creation (e.g., in progress or ongoing), as well as when the POA&M is delayed and when it is completed. Approves all POA&Ms at any priority when the status is changed to delayed, waiver, or cancelled. Conducts quarterly reviews of the consistency and accuracy of the Component's POA&M data Ensures, within their Component, that IACS is used to develop, track, and manage the remediation of IT system and program weaknesses Implements and manages a POA&M process for remediation by ensuring that a POA&M is created for each vulnerability. Ensures that ISSOs are appointed for each information system managed at the Component level. Ensures training for and oversight of personnel with significant responsibilities for information security.
Component Chief Financial Officers (CFOs)	Serves as AO for all financial systems managed by the Component. Implements and manages the DHS Financial Program, including oversight of DHS financial systems. Designates financial systems and oversees security control definitions for financial systems. Approves all POA&M waiver and exception requests related to CFO designated systems.
Authorizing Officials (AOs)	Ensures that POA&Ms are developed for all identified weaknesses except those where a decision has been made to accept the risk. System Owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced, and documented in accordance with current OMB budgetary guidance.
Common Control Providers	Is responsible for planning, development, implementation, assessment, authorization, and maintenance of common controls. Ensures that POA&Ms are developed for all common controls having weaknesses or deficiencies. Makes available security plans, Security Assessment Reports (SARs), and POA&Ms for common controls to information system owners inheriting those controls after the information is reviewed and approved by a senior official.

Role	Responsibility
System Owners	Responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. While the ISSO performs security functions, the System Owner is always responsible for information system security. Ensures development of a POA&M to address weaknesses and deficiencies in the information system and its environment of operation which remain after Security Authorization. System Owners or AOs ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.
Information System Security Officers (ISSOs)	Perform security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. A system can have only one ISSO, but that does not preclude an ISSO from having multiple systems. While the ISSO performs security functions, the System Owner is always responsible for information system security. Designated for every information system and serve as the point of contact (POC) for all security matters related to that system. Ensure the implementation and maintenance of security controls in accordance with the Security Plan (SP) and DHS policies. Work with system owners and other stakeholders to develop, implement, and manage corrective action plans for all systems they own and operate For systems under their control, ensure that POA&Ms are created for every IT security weakness and entered into IACS. Develop, track, and manage POA&Ms for systems under their control Ensure that POA&Ms are updated in IACS Ensure that Component POA&Ms contain appropriate details as required by DHS 4300A Attachment H.
System Administrators	Work with Component ISSOs to develop, implement, and manage system level corrective action plans for all systems that support their operations and assets Provide regular updates on the progress of remediation for weaknesses
Program Managers/Officials	Responsible for program-level POA&Ms that may impact one or more systems. Provide copies of program POA&Ms to affected System Owners. Ensure that POA&Ms address the following: Known vulnerabilities in the information system The security categorization of the information system The specific weaknesses or deficiencies in the information system security controls The importance of the identified security control weakness or deficiencies The Component's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls

APPENDIX H11 SEVERITY LEVEL DETERMINATION

The determination of severity level should be a carefully considered risk-based decision.

The management decision to define the severity level of a weakness is supported by a risk-based approach. The questions to consider are:

- What is the system's categorization?
- What is the NIST 800-53 control family?
- Is the weakness system specific or is it a Common Control weakness?
- What is the severity of the weakness according to OMB POA&M Instructions?
- What is the NIST 800-30 impact level?

The appropriate urgency and resources are better aligned and applied when risk, impact, and severity of a weakness are assessed during remediation planning, then an effective and efficient plan for corrective action can be documented as a POA&M and executed within the scheduled completion date.

Steps to consider in determining the risk level of a weakness

1. Begin by knowing the FIPS 199 system categorization of the system being reviewed.
    - Under system categorization, the highest rated security objective drives selection.
    - Review with the FIPS 199 impact definition of the highest control objective for the weakness. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
2. Understand the impact level, which is based on the CNSSI No. 4009 definition of impact level.
    - Impact level is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information (**confidentiality**), unauthorized modification of information (**integrity**), unauthorized destruction of information, or loss of information or information system availability (**availability**).
    - The impact level has **an impact value** that is based on the CNSSI No.1253 definition and is expressed as a value of low, moderate, or high.
    - The assessed potential impact resulting from a compromise of the confidentiality integrity, or availability of an information type, expressed as a value of low, moderate, or high.

What is the system's categorization?

High = 4 points	Any combination with high in the category is high.
Medium = 3 points	Any combination with medium in the category is medium.
Low = 2 points	Any combination with low in the category is low.

What is the NIST 800-30 impact level?

Very high = 6	Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High = 5	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national.
Moderate = 4	Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low = 3	Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very low = 2	Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Is the weakness system specific or is it a Common Control weakness?

System specific	4
Common Control	5

The OMB definition of risk, and the NIST impact levels, are as follows:

Risk level is dependent on multiple factors, such as the Federal Information Processing Standard (FIPS) 199 category, operating environment, compensating controls, nature of the vulnerability, and impact if a system is compromised. If no risk level has been assigned, the process described in NIST SP 800-30 may be used to help determine the proper risk level of a weakness. NIST SP 800-30 provides a foundation for the development of an effective risk management program; it contains both the definitions as noted in Table 1 and the practical guidance necessary for assessing and mitigating identified risks to IT systems.

DHS assigns priority based on the risk level of a weakness. NIST) Special Publication (SP) 800-30, "Guide for Conducting Risk Assessments," and NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," defines risk as a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are essential to continuity of government operations.

Each identified weakness poses some level of risk to the system and the mission it supports. Risk is the likelihood that a threat-source could exploit vulnerability and cause an adverse impact on the organization. To better understand the overall risk, assign a risk level to the weakness while keeping in mind the FIPS 199 assigned risk level for the information system.

Table 1: Risk Scale, delineates the risk scale used at DHS.

Risk Level	Risk Description and Necessary Management Action
HIGH	If an observation, weakness, or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
MODERATE	If an observation, weakness, or finding is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
LOW	If an observation, weakness, or finding is described as low risk, the corrective action is still required within remediation time limits.

Table 1: Risk Scale

High Risk: indicates that a serious incident is likely. High risks are not normally acceptable according to the system sensitivity and criticality.

Moderate Risk: indicates that an incident has an elevated probability of unauthorized disclosure of a critical system.

Low Risk: indicates that the risk is not as impactful in the short term until cost-effective safeguards can be implemented. Low risk deficiencies should be remediated.

Management (including AO, ISSM, and system owner) can raise the priority level above the finding category. The following tenets should be observed as to prioritization:

- If a weakness identified during the Security Authorization process (formerly C&A process) is considered a high risk that must be resolved expeditiously, it should be listed as a priority 5 (IV) "management decision."
- Management should prioritize weaknesses from any other source at the appropriate level as given in Table 3's Designated Category column.
- To ensure adequate risk accountability, only management has the authority to declare a higher risk level than formally assigned.
- Any weaknesses that do not fall within one of the specified categories (for example, vulnerability scans) should be listed at the appropriate level as a management decision.

Weaknesses that are identified from multiple sources are prioritized at the highest source level. For example:

- If a weakness is found in the Security Authorization process, it is assigned a minimum priority level of 3
- If this weakness is later identified in an audit, it becomes a priority level 4 since audit findings have a higher priority than Security Authorization findings
- If this weakness is later found in an annual assessment, it will remain at a priority level 4. as it is still the highest priority

APPENDIX H12 CISO/ ISSM VALIDATION CHECKLIST

Activity	Review /Monitor / Validate
Root Cause Analysis	Review all POA&M aspects to determine that the collaborative remediation strategy that was conducted with stakeholders to determine the root cause of the weakness will be executed effectively and will be remediated timely based on the plan of action schedule.
Milestone Creation	Review milestones when created to ensure the following: A milestone is required to test for effectiveness, which refers to verifying that the control actually performs as intended and is consistent with the design. **Required for financial and non-financial systems**, in addition to the milestones for the plan of action for remediation. A milestone is required to test for design of the control, which refers to the documented process or procedure that implements the control. **Required for financial systems**, in addition to the milestones for the plan of action for remediation. Optional, but preferred for non-financial systems. The milestone should effectively communicate the major steps that will be performed to correct the weakness. The milestone scheduled completion dates should be incremental as a project plan would be. All dates should not be the same because all activities would not begin and end at the same time. The plan of action would fall behind schedule if the activities described in the milestones do not show progression to move toward completion.
Artifacts	The finding document should be uploaded as an artifact to review the official cause and recommendation from the review or audit to determine if the plan of action will remediate the weakness. Evidence of the percent complete should be uploaded as an artifact to support the progress made.
Milestone Status Monitoring	Review milestone status reports monthly to determine if the plan of action to remediate is on schedule. If milestone activity is not being performed based on observation that the status is not being updated at least every 30 days, determine why progress is not being made and what will get the plan back on schedule.
Approvals	Validation is required for the following statuses: Complete – review uploaded artifact and remediation test results to ensure that it supports complete status Delayed Cancelled Waiver

APPENDIX H13 DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 29, 2005	Initial release
4.0	June 1, 2006	Verification of references. Minor editorial changes
5.0	March 1, 2007	Updated content throughout
6.0	May 14, 2008	New or updated content 1.3 National security systems 2.2 ISSM responsibilities 3.1 Incident report inclusion in POA&Ms 3.3 Prioritization 3.4 Developing milestones 4.2.1 Weakness description 4.2.4 Waivers and exceptions 4.2.5 Delayed and overdue POA&Ms 4.2.7 Milestones 4.2.8 Audit ID 4.2.10 New status categories 4.3 Requirement to add Control Titles 5.1 Reports 6.1 FY08 scorecards Appendix D - POA&M checklist Appendix F - Reasonableness criteria. Updated table to align with NIST SP 800-53 Revision 1
6.1	September 23, 2008	New or updated content 2.2 Updated ISSM responsibilities for approving POA&Ms 3.4 Added guidance on root cause analysis 4.2.1 Added guidance on audit recommendations in POA&Ms 4.2.7 Added guidance on the number of milestones that should be included in POA&Ms and a new requirement for test milestones for financial audit findings. 4.2.9 Described the recommendation number function in the TAF Identified In window 4.2.10 Described the Draft status in TAF and clarified the difference between waiver and exception statuses. 4.2.11 Added guidance for use of Control Titles in POA&Ms 4.5 Added guidance on for POA&Ms for classified systems Updated Appendix F - Reasonableness criteria Added Appendix G - Weakness Search Report Guide Added Appendix H – Root Cause Analysis Guide

Version	Date	Description
6.2	February 15, 2009	New or updated content 1.3 Added details regarding use of TAF/C for classified system POA&Ms 2.2 Added responsibilities for CFO 3.1 Identified new sources of weaknesses to be reported 3.3 Added priorities for new sources of weaknesses 4.2.1 Clarified weakness description requirements 4.2.9 Added guidance for recording data in the "identified In" field in TAF 4.5 Added details regarding use of TAF/C for classified system POA&Ms 5.1 Added details regarding availability of daily reports 6.2 Changed help desk contact information Update Appendix D to reflect changes throughout document Updated Appendix F to remove schedule criteria for reasonableness Update Appendix G to reflect changes throughout document Updated all figures to reflect changes in TAF
7.1	October 1, 2009	New or updated content Added determining risk level to the POA&M Process 3.3 Added a new section regarding how to determine risk level 3.7 Added sentence regarding CISO function to review POA&Ms and fail them if they are non-compliant 4.1 Updated TAF helpdesk POC info 4.2.1 – 4.2.26 Expanded definitions of POA&M data elements. 4.2.25 Updated procedures for entering milestones in TAF 4.2.7 Expanded descriptions of status options in TAF and provided guidance on when to use each 4.2.20 Expanded guidance for use of control titles for 4300A controls Table 3 Added A-123 reviews and CCR Appendix A Updated to be consistent with 4300A Appendix C Added risk elements and priority options Appendix F provides sample weaknesses and milestones Appendix G Updated reasonableness matrix to include new NIST SP 800-53 rev 3 controls Added Appendix F Sample Weakness Descriptions and Milestones Updated and reordered Appendices to be consistent with text Added Section 3.3 on assigning Risk to weaknesses Updated figures to reflect changes in IACS
9.1	June 2012	Document updated by the CISO Compliance Division. Principal changes were: Moved Document Change History to end of document Added POA&M Definition and Purpose Added section to provide a more in-depth description of CPIC; Figure 1 added highlights to capital planning screen shot Updated POA&M roles and responsibilities to align with DHS 4300A Sensitive Systems Policy Directive Risk levels applied to Common Controls Common Control is added to Criticality (Priority) and the Identified In data elements Increased emphasis placed on the importance of determining root cause Added glossary to Appendix H1 The section on Financial Systems has been added to the table of contents due its level of importance and uniqueness. The naming convention for the Report ID data element has been added for clarity and consistency Stylistic and formatting changes throughout the document.

Version	Date	Description
9.1	September 2012	Document updated by the CISO Compliance Division. Principal changes were: Inserted list of figures and list of tables Inserted screenshot of the My Tasks Daily TAF Report in Section 4.8 Added milestone requirement for non-financial systems in Section 6.2.25 Inserted screenshots of the Milestone Status update data elements in Section 6.2.26 Added clarification on the definition of the TYPE data element in Section 6.2.13 Stylistic and formatting changes throughout the document
10.0	February 2014	Removed TAF references that described process steps. Removed TAF icons such as the red ellipse button that was no longer applicable. Removed screenshot figures from the TAF version of IACS. Inserted data element crosswalk to transition from TAF version of IACS to the XACTA version of IACS in Section 6.2, Required POA&M Data. Changed processes to align with the XACTA version of IACS. Removed processes that were no longer applicable due to change to XACTA version of IACS such as Appendix H9, Weakness Search Report Guide since the reporting process described in TAF is no longer applicable.
11.0	December 3, 2014	Entire document revised to accommodate the POA&M tool change from TAF to IACS.