IT Security Procedural Guide: Plan of Action and Milestones (POA&M) CIO-IT Security-09-44

Revision 8

September 14, 2022

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORDS

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 - 2011		
1	Berlas	Changes throughout the document to reflect FY11 reporting schedule.	Annual Review	Various
1	Berlas	Attached the FY11 POA&M template.	Annual Review	8
		Revision 2 – 2013		
1	Jones	Updates for FY 13 POA&M requirements to include, FISMA Google site procedures, Quarterly Management Report, and Annual Recertification Process.	Annual Review	Entire Guide
		Revision 3 – June 29, 2016		
1	Jones/ Klemens	FY16 POA&M updates w/new template revisions	Annual Review	Entire Guide
		Revision 4 – February 23, 2017		
1	Dean/ Klemens	FY17 POA&M updates w/new template revisions	Annual Review	Various
		Revision 5 – January 19, 2018		
1	Akinniyi/ Dean	FY18 POA&M process updates w/new template revisions.	Annual Review	Various
		Revision 6 – April 6, 2020		
1	Morgan/ Dean	FY20 POA&M process updates: • Incorporate template revisions • Information regarding funding Column in POA&M template • Added AOR requirements • Clarified when POA&Ms are required for EOL software, audit findings (aligned with 06-30) • Added responsibilities for ISSO and ISSM regarding ISSO checklists in Archer • Updated information vulnerability timelines (aligned with 06-30) • Added on POA&Ms regarding Cybersecurity Directives • Updated POA&M review process	Annual Review and update to reflect updated policy and guidance.	Various
		Revision 7 – August 25, 2021		
1	Klemens/ Morgan	Updates to address FY21 process: • Incorporate template revisions • Updated references and dates, as applicable	Updates to reflect updated processes and guidance.	Various
		Revision 8 – September 14, 2022		
2	McCormick/ Klemens	Revisions include: • Updated NIST SP 800-53 references • Minor editing and updating of format and style. • Updated links, as applicable	Update to current NIST references and guide format and style.	Various

Approval

IT Security Procedural Guide: Plan of Action and Milestones (POA&M), CIO-IT Security 09-44, Revision 8, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

Notes:

- Hyperlinks will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Section 1.3.
- It may be necessary to copy and paste hyperlinks found in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

The Plan of Action and Milestones (POA&M), also referred to as a corrective action plan, is the authoritative agency management tool for documenting the remediation actions of system risk. POA&Ms are used to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems. This guide addresses both program and system level POA&Ms. Additional information about program POA&Ms and GSA's enterprise level information security program is available in CIO-IT Security-18-90: Information Security Program Plan.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" provides Federal guidance on POA&M management, monitoring, and reporting requirements. The General Services Administration (GSA) requires POA&M updates to document the progress of the remediation efforts associated with identified weaknesses, including schedule changes. The GSA Office of the Chief Information Security Officer's (OCISO) Policy and Compliance Division (ISP) reviews POA&Ms on a quarterly basis.

POA&Ms must:

- Estimate funding required to remediate the action if existing operation and maintenance (O&M) or development, modernization, and enhancement (DME) will not be used.
- Include security weaknesses in need of remediation identified during any assessment. For details on the types of assessments, audits, and categorization of POA&Ms see Section 5 and CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk. POA&Ms are an authoritative agency-wide management tool used to address findings from all evaluations.
- Be made available or access provided to the Office of Management and Budget (OMB), Department of Homeland Security (DHS), GSA Inspector General (IG), and GAO upon request.
- Record and manage the mitigation and remediation of identified weaknesses and deficiencies, not associated with accepted risks, in organizational information systems and environments of operation.
- Record the status of delays (30, 60, 90, and 120 or more days).
- Be a permanent part of the A&A documentation for the life of the IT resource.

1.1 Purpose

This guide provides GSA employees and contractors with significant security responsibilities as identified in the latest version of the GSA CIO Order 2100.1, "GSA Information Technology (IT)

Security Policy," with the necessary guidance and procedures for developing, maintaining, and reporting POA&Ms for systems and programs under their purview.

The purpose of a POA&M is to monitor progress in correcting weaknesses or deficiencies associated with information systems. The POA&M identifies: (i) the tasks to be accomplished; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) scheduled completion dates for the milestones. Detailed instructions on completing POA&Ms are contained in the POA&M Instructions Google Doc.

A risk assessment must be performed and the results leveraged to prioritize the remediation of the entries included within the POA&M. This will help ensure the weaknesses are addressed in a timely manner and receive appropriate resources.

In the event a risk cannot be remediated an Acceptance of Risk (AOR) must be created and properly approved in accordance with GSA CIO-IT Security 06-30, "Managing Enterprise Cybersecurity Risk."

1.2 Policy

As required by Public Law 113-283, "Federal Information Security Modernization Act of 2014" (FISMA), the GSA information security program provides security for information and information systems that support the operations and IT assets of the agency.

The processes presented in this guide reflect requirements defined in Public Law 113-283, CIO Order 2100.1 and NIST SP 800-37, Revision2.

GSA CIO 2100.1, Chapter 3, Policy for Identify Function, states:

4. *Risk assessment.*

   h. All information systems must develop and maintain a POA&M IAW GSA CIO-IT Security-09-44. POA&Ms are the authoritative agency management tool for managing system risk and are used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems.

GSA CIO 2100.1, Chapter 4, Policy for Protect Function, states:

4. *Information protection processes and procedures.*

   cc. The OCISO will review POA&Ms quarterly and provide system level and management reports IAW GSA CIO-IT Security-09-44.

1.3 References

Federal Laws, Standards, Regulations, and Publications:

- NIST Interagency or Internal Report (NISTIR) 7298, Revision 3, "Glossary of Key Information Security Terms."
- NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- OMB Circular A-11, Capital Programming Guide, Supplement to Part 7.
- Public Law 113-283, "Federal Information Security Modernization Act of 2014"

GSA Policies, Procedures, Guidance:

The GSA policy listed below is available on the GSA.gov Directives Library page.

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-18-90 which is restricted. It is available on the internal GSA InSite IT Security Procedural Guides page.

- CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk"
- CIO-IT Security-09-44, "Plan of Action and Milestones (POA&M)"
- CIO-IT Secuity-18-90, "Information Security Program Plan"

Additional GSA Resources (restricted access):

The GSA forms listed below are restricted and available on the internal GSA InSite IT Security Forms and Aids page.

- POA&M Shared Drive User Access Request Form FY22 V3
- Security Deviation/Waiver Request Form

The GSA resources listed below are restricted and available on internal GSA Insite pages.

- POA&M Instructions Google Doc
- GSA FISMA Systems – POC
- GSA IT System Inventory

1.4 Quarterly POA&M Reporting Schedule

Unless directed otherwise by the OCISO, the Fiscal Year review dates performed by ISP are:

- Q1 – December 1;
- Q2 – March 1;
- Q3 – June 1;
- Q4 – September 1.

ISP sends one reminder per quarter regarding upcoming POA&M reviews, which also identifies any POA&M entry or reporting changes required. The submission schedule may also be located on the POA&M Guidance Google Shared Drive.

ISP provides the ISSMs with a listing of system POA&Ms not received for review approximately one week following the quarterly due date.

2 Roles and Responsibilities

The roles and POA&M responsibilities provided in this section have been extracted from GSA CIO 2100.1 or summarized from Federal guidance. Throughout this guide specific processes and procedures for implementing the GSA POA&M Management Program are described.

2.1 GSA Chief Information Officer (CIO)

Responsibilities include the following:

- Developing and maintaining an agency-wide GSA IT Security Program.
- Providing management processes to enable the Authorizing Official to implement the components of the IT Security Program for which they are responsible.
- Reporting annually, in coordination with the other senior agency officials, to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.
- Providing guidance or input for periodic assessments of Service and Staff Office's (SSO) security measures and goals to assure implementation of GSA policy and procedures.
- Providing direction and coordinating with senior agency staff throughout the year on a comprehensive POA&M process.

2.2 GSA Chief Information Security Officer (CISO)

Responsibilities include the following:

- Establishing reporting deadlines for IT Security related issues requiring an agency response affecting the GSA IT Security Program.
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.
- Supporting the GSA CIO in reporting to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.
- Developing and implementing IT security performance metrics to evaluate the effectiveness of technical and nontechnical safeguards used to protect GSA information and information systems.
- Administering FISMA requirements and coordinating GSA's annual FISMA security program review and Plan of Action and Milestones (POA&M) implementations.
- Managing and maintaining the agency POA&M process and tools.

- Providing guidance to SSO AOs, ISSMs, ISSOs, System Owners and others in maintaining their POA&Ms in accordance with GSA and Federal policies.
- Establishing the process for POA&Ms to be reviewed and reports to be prepared on a quarterly or ad hoc basis.

2.3 Authorizing Official (AO)

Responsibilities include the following:

- Ensuring a formal POA&M has been developed following an A&A process.
- Ensuring vulnerabilities identified from scans are tracked in the systems' POA&M as required by the OCISO.
- Ensuring POA&Ms are managed and maintained via the agency's POA&M process using tools identified by the OCISO.
- Reviewing POA&M metrics or reports and responding, as appropriate.

2.4 Office of the Chief Information Security Officer (OCISO) Directors

Responsibilities include the following:

- Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO.
- Providing guidance and support to the ISSMs and ISSOs for the management and maintenance of POA&Ms.

2.5 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Ensuring adherence and proper implementation of GSA's IT Security Policy.
- Managing POA&Ms for all systems under their purview. This includes ensuring quarterly updates are submitted on time.
- Ensuring ISSOs and System Owners are maintaining POA&Ms for their systems, including taking remediation actions according to the scheduled milestones.
- Authorizing POA&M Shared Drive User Access Request Forms or authorizing access via an email for individuals supporting the POA&M process when appropriate.
- Reviewing POA&M metrics and reports (see Section 7.2) and responding in a timely manner, as appropriate.
- Reviewing/approving ISSO checklists submitted in Archer GRC with respect to POA&Ms, and coordinating with ISSOs, as necessary, for systems under their purview.

Note: ISSMs should ensure POA&Ms are being updated prior to quarterly reporting; and provide training to ISSO, and System Owners on proper POA&M reporting.

2.6 Information System Security Officer (ISSO)

Responsibilities include the following:

- Ensuring effective implementation of GSA's IT Security Policy.
- Working with the ISSM and System Owners to develop, implement, and manage POA&Ms for assigned systems.
- Ensuring the POA&M is a permanent part of the A&A package, per GSA requirements. POA&Ms should never be deleted.
- Submitting accurately updated POA&Ms in a timely manner as required.
- Reviewing POA&M metrics and reports (see Section 7.1) and responding in a timely manner, as appropriate.
- Documenting the review/update of system POA&Ms when completing assigned ISSO checklists in Archer GRC and submitting the checklists when completed.

2.7 System Owners

Responsibilities include the following:

- Ensuring effective implementation of GSA's IT Security Policy.
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems as required by GSA policy.
- Reviewing POA&M metrics and reports and responding in a timely manner and as appropriate.
- Prioritizing the Top 5 POA&M weaknesses by criticality (i.e., weaknesses with the greatest potential impact to the organization's mission are addressed first).
- Assuring resources are allocated to POA&Ms with the greatest criticality.

3 POA&M Shared Drives

ISP tracks all GSA POA&Ms on Google Share Drives which serve as the primary tool for the management, storage, and dissemination of GSA program and system level POA&Ms.

3.1 Access to Shared Drive

ISSOs, and ISSMs listed on designation or ATO letters will be provided access to POA&Ms for systems under their purview. System Owners identified in the GSA System Inventory will be provided comment access to view POA&Ms for the systems under their purview. Any person who is not provided access via a designation or ATO letter must complete a POA&M Shared Drive User Access Request Form to the ISSM for approval to access a system's Shared Drive. This access request form is to be authorized by the ISSM of the system. Once authorized, the form should be sent to OCISO ISP at ispcompliance@gsa.gov.

3.2 Shared Drive Directory Structure

System POA&Ms and related data are located on Google Shared Drives. System POA&Ms are in individual Shared Drives with the following naming convention: POA&M – [Service and Staff Office (SSO Code)] – ISSM - [ISSM Name] – [System Name]. ISSOs, and others as authorized, will be able to access their systems' Shared Drives to maintain POA&Ms, and provide additional documents/data as required. Figure 3-1 depicts a generic example of a Shared Drive structure. Systems scanned for vulnerabilities by GSA's internal scanning processes may not have a scans folder as depicted.

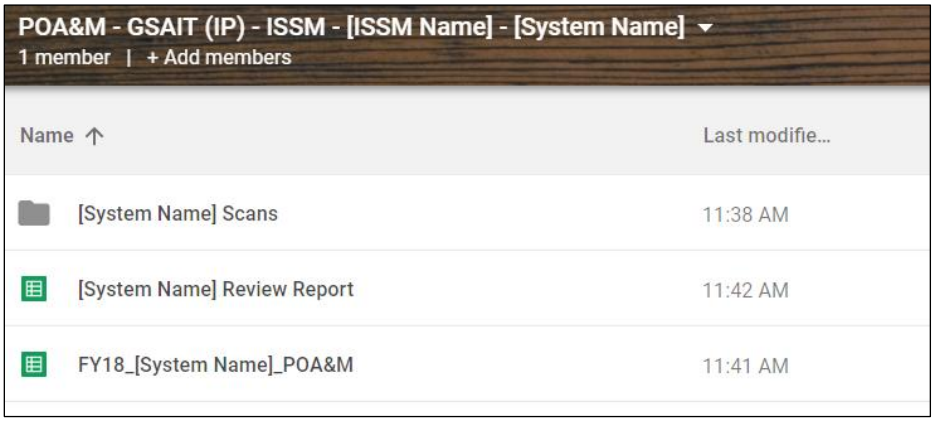

Figure 3-1: Shared Drive Structure

3.3 Annual Shared Drive Access Recertification Process

User access to the POA&M Shared Drives must be recertified annually. Based on the persons identified in the GSA FISMA Systems – POC (internal webpage) listing, a recertification email will be sent to each ISSM with a link to a Google drive document identifying all current users with access to each POA&M Shared Drive. The ISSM must verify those persons who have access for each system under their purview. This process may require updated designation letters be provided to ISP. Once the ISSMs have verified current users the Shared Drives will be updated to reflect access changes. Access will not be recertified by default; proper authorization by the ISSM must be provided.

4 POA&M Types

GSA uses two types of POA&Ms, Program Level and System Level. Unless specified otherwise within this guide, the creation, management, and reporting of Program and System Level POA&Ms is the same.

4.1 Program Level POA&Ms

A Program Level POA&M assists a SSO in documenting Program Management Office (PMO) weaknesses or deficiencies at the program or GSA organization level which affect the program's

or organization's IT security efforts. The remedial actions defined reduce or eliminate identified weaknesses or deficiencies in the operation of programs for an organization.

4.2 System Level POA&Ms

A System Level POA&M assists in documenting planned remedial actions to correct weaknesses or deficiencies identified in relation to the technical, management, or operational aspects of a GSA system, IT resource, or controls in, NIST SP 800-53, Revision 5.

5 POA&M Criteria

5.1 Systems Requiring POA&Ms

All GSA FISMA systems in the GSA IT System Inventory are required to develop, manage, and maintain a corresponding POA&M. Subsystem POA&Ms will be entered and maintained within the hosting information system's POA&M. The subsystem must be listed in the hosting information system's Hosted Subsystems appendix in its SSP, and its ATO letter.

5.2 POA&M Weakness Tracking Requirements

System weaknesses identified by the following sources must be documented in the POA&M within one quarter of identification. ISP strongly suggests that POA&M updates be entered when the status of an entry changes and not just when quarterly submissions are due for review. All findings based on audits must be completed within twelve months of entry in the POA&M.

The following sources of weaknesses must be included in POA&Ms:

- **GAO Audits.** All findings noted in the final report, including those that may have already been corrected, must be individually identified in the POA&M.
- **Office of Inspector General (IG) Audits.** All findings noted in the final report, including those that may have already been corrected, must be individually identified in the POA&M.
- **Annual Financial System Audits.** All findings noted in the final report, including those that may have already been corrected, must be individually identified in the POA&M.
- **Internal Audits/Third Party Assessments.** Findings noted in internal audits, third party assessments, or other reviews, as applicable, must be individually identified in the POA&M.
- **Annual FISMA Self-Assessments.** All weaknesses from an annual FISMA self-assessment, subject to the following criteria, must be included. Repeat finding(s) from prior years that are already reflected in the POA&M do not have to be re-entered. Update the *Weakness Source* column with the existing finding(s) to document the finding with the current year FISMA self-assessment. Update

milestone changes, as appropriate. A prior entry not completed by its completiong date must reflect the status as delayed.

- **Assessment and Authorization (A&A).** Include vulnerabilities of the information system discovered during the A&A process and/or security continuous monitoring as follows.
  - POAMs from a SAR
    - Do not create POA&Ms for any vulnerabilities identified as "Remediated" or "False Positive" in the SAR.
    - Create POA&Ms for all other vulnerabilities (including scan findings) in the SAR as individual POA&Ms.
  - POA&Ms from other assessments adhere to the following conventions:
    - All findings from audits become individual POA&Ms.
    - All findings indicating End-of-Life (EOL) software or components become individual POA&Ms.
  - Vulnerability Scans
    - If vulnerabilities in the Cybersecurity & Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog cannot be readily corrected within the KEV timeline an additional 14-day grace period will be given. After this period, the CIO and AO will have the option of approving the creation of a POA&M for no longer than 60 days beyond the KEV's remediation date.
    - POA&Ms must be created for vulnerabilities exceeding the remediation timelines listed below.
      - 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
      - 30 days for Critical (Very High) and High vulnerabilities.
      - 90 days for Moderate vulnerabilities.
      - 120 days for Low vulnerabilities for Internet-accessible systems/services.
    - External vendor/Contractor systems: Low vulnerabilities must have POA&Ms established within 90 days, although there is no remediation deadline (other than as listed above).
  - Configuration/Compliance Scans. A FISMA system must monitor compliance to all the configuration settings required by GSA hardening guides. Each configuration setting must be covered by one of the following clauses:
    - The configuration setting is compliant; the asset's setting is either
      - Equal to the setting required, or
      - More restrictive than the setting required.

- The configuration setting is not compliant - The asset is configured with a more liberal setting than required. In this case, the non-compliant configuration setting needs to be accounted for in one of the following ways:
  - Deviation - The non-compliant setting is covered by an approved deviation.
  - POA&M - If the composite compliance percentage of all assets with a single operating system is below 85% for over 90 days, a POA&M must be created for the non-compliant operating system. The resultant POA&M will state:

    "Configuration/compliance scans indicate that [ENTER OPERATING SYSTEM] has been below 85% compliant for over 90 days."

Note: GSA systems not being scanned under GSA's vulnerability scanning program must include all identified weaknesses in their POA&Ms to provide GSA OCISO with visibility into their vulnerabilities. Supporting scan reports must be provided to the OCISO ISP division as part of updating the POA&M via the POA&M Google Shared Drives. Scan folders are located inside of appropriate system Shared Drives for ISSO to upload vendor provided scans.

- Cybersecurity Directives**.** All binding operational directives (BODs) and emergency directives published by the Department of Homeland Security (DHS) where a system is not compliant must be identified in the system's POA&M.
- GSA systems undergoing reauthorization must document any new A&A findings into the existing POA&M on their Google Shared Drive. A system's POA&M is a permanent part of the A&A documentation package. Completed entries may be filtered out to reduce the visible size of the document but must not be removed. Certain columns as specified in the POA&M Instructions have been identified and must not be changed.
- Acceptance of Risk (AOR) letters and corresponding POA&M entries associated with them must be completed in accordance with CIO-IT Security-06-30.

5.3 Additional Information Regarding POA&Ms

Sensitive descriptions of specific weaknesses are not necessary, but sufficient data is necessary to permit oversight and tracking. To the maximum extent practicable, use the types of descriptions commonly found in GAO and IG reports. Terms such as "inadequate password controls," "insufficient or inconsistent data integrity controls," "inadequate firewall configuration reviews," "background investigations have not been performed prior to system access," "physical access controls are insufficient," etc. should be used. Where it is necessary to provide more sensitive data, the POA&M should note its special sensitivity. If detailed weakness/milestone information that is actionable cannot be provided due to potentially sensitive vulnerabilities, indicate where the detailed weakness may be located in the supporting audit report. Input this information in the *Weakness Source* column.

The OCISO/IST division should have a copy of the audit report. This report should be maintained as a permanent part of the system's ATO package.

POA&M entries must not be removed from the POA&M. POA&M updates should be documented in Column K*, "Milestone Changes."* Updates are made when there is a change to the initial weakness information. Completed weaknesses may be filtered from view by the OCISO ISP division during the last POA&M update of the fiscal year. This assures that actions are auditable and traceable

Weaknesses transferred from one system POA&M to another must be clearly traceable and justified. Transferred weaknesses should be documented in Column K, "*Milestone Changes*." Enter the purpose for the transfer, the title of the new POA&M, and the ID number of the new weakness.

Using "To Be Determined (TBD)" for scheduling completion dates must be avoided. If a TBD status is required, a rationale must be provided in Column R*, "Rationale."* A TBD status can only be used for one quarter.

Deviations must be submitted with the POA&M. If the status of a POA&M item is Deviation Requested or Deviation Approved, the Request/Approval must be submitted using the Security Deviation/ Waiver Request Form.

6 POA&M Template Content and Guidance

Weakness information is gathered and reported using the most current GSA POA&M Template.

The Google Sheet POA&M template contains five sheets (tabs), consisting of:

- System POA&M Metrics sheet (Tab 1);
- POA&M sheet (Tab 2);
- Instructions sheet (Tab 3);
- FAQ sheet (Tab 4); and
- FY Compliance Initiatives sheet (Tab 5).

The OCISO ISP Division updates the POA&M template annually and transitions existing entries into a new template, and places one in each system's Shared Drive. Annual updates are provided at the start of the fiscal year prior to the Q1 POA&M review. New systems must use the current FYXX POA&M template available on the POA&M Guidance Shared Drive. POA&Ms must be prepared and submitted by ISSOs/ISSMs or approved designated personnel. POA&Ms must be updated when there is a significant change or an entry has been resolved. Quarterly tabs must be updated to document any delay status of existing entries.

For guidance on how to use the POA&M template, review the POA&M Instructions Google Doc.

6.1 POA&M Sharing

6.1.1 Sharing with Non-Shared Drive Members

If there is a requirement to share a system's POA&M spreadsheet with GSA account holders who should not have access to the entire Google Shared Drive, share the POA&M manually:

1. Ensure the ISSM has been made aware the POA&M is being shared.
2. Right click on the POA&M file and select "Share."
3. Enter the name/email address of the user to be granted access to the POA&M.
4. On the Pencil icon dropdown, select the user's permissions (Viewer, Commenter, Editor) for the Google Sheet, and other options as appropriate.
5. Always notify individuals when access has been provided.
6. Click on "Done."

Note: Leave the General Access status set to "Restricted." Do not open up access to gsa.gov.

Once these actions are completed, verify the correct access was provided.

6.1.2 Sharing with Non-GSA Account Holders

If there is a requirement to share a system's POA&M with non-GSA account holders, take the following actions.

1. Ensure the ISSM has been made aware of the access request and when the action occurs.
2. Download the POA&M; this will convert the POA&M to a Microsoft Excel spreadsheet.

   Note: The conversion does not impact the data or formulas in the POA&M file. However, the conversion does cause the dashboard graphics on the System POA&M Metrics tab to display differently than in the Google Sheet (Wordwrap and sizing of charts does not translate well in all cases).

3. Share the POA&M as necessary. A link to the POA&M instructions (this document) is included in the POA&M template. Since non-GSA account holders will not have access to the instructions document, it will need to be downloaded and shared.
4. Data that has been updated in the Excel POA&M will need to be integrated into the POA&M on the Team Drive by following the steps in the Copy and Paste Between POA&M Spreadsheets section of the POA&M Instructions Google Doc. The ISSO is responsible for ensuring the data has been accurately integrated into the POA&M and neither the data nor formulas/conditional formatting has been corrupted. The ISSM must verify the updates prior to the quarterly review process.

Note: The original POA&M Google Sheet must not be replaced by another Google Sheet or by uploading an Excel spreadsheet that has been converted to a Google spreadsheet. Doing so will cause existing reporting functions in other sheets to malfunction and report incorrect POA&M information.

7 POA&M Reviews and Reports

This section describes the processes used to review POA&Ms and report on those reviews.

Note: All Management Reports described in the following sections are created only during the quarterly reviews of POA&Ms.

7.1 POA&M Review and Report (ISSO)

Unless otherwise indicated ISP will review POA&Ms upon initial A&A of a GSA system (i.e., when an ATO Letter is received) and quarterly thereafter. ISP will provide comments in a POA&M Review Report which will be contained in the system's folder under the applicable Shared Drive. The ISSO/submitter will be notified when the review report has been completed. Comments must be mitigated and/or addressed within one (1) week of the report date. After the POA&M has been updated based on ISP comments, the ISSO/submitter should notify the ISP analyst who completed the review.

Note: POA&M reviews will be conducted using the system documents in the Archer A&A Repository and the information in the IST ISSM Assignment & Risk Tracking Google Sheet. The documents and information in these two sources should be current at all times.

7.2 Management Report (ISSM/System Owner)

Approximately one week from the distribution of a quarterly ISSO POA&M Review Report, an ISSM Management Report will be available to ISSMs. An ISSM Management Report is a single Google spreadsheet that consists of multiple tabs distributed by ISSM and SSO with a compilation of GSA IT SSO system information taken from the quarterly POA&M reviews and made available to the ISSMs. Once the management report is complete, notification will be sent to the ISSMs, copying the ISSOs. The report will be available on the applicable POA&M Shared Drive. The ISSMs will have approximately one week from the date of distribution to make any changes and finalize their documents. Once finalized, the applicable quarter's data in the management reports cannot be edited.

7.3 Management Report (Director)

Approximately one week from the distribution of the quarterly ISSM Management Report, a Director Management Report with applicable updates will be provided to the IST Director and the ISSMs. The Directors Report reflects the final status of the ISSM reports. The IST Director will have one week from the time of receipt to take any action before the Final Management Report is sent to the CISO/AO's.

7.4 Management Report (CISO/AOs)

Approximately one week from the distribution of the quarterly Director Management Report, the CISO/AO's Management Report will be prepared and provided to the CISO. This report

reflects the final status of the Directors Report, including a summarization of pertinent POA&M metrics. The report will be shared with the AO at the CISO's discretion.

8 Definitions

Definitions marked with an * have been extracted from National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 7298, Revision 3.

Assessment/Security Control Assessment*
The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system and/or enterprise.

Authorization (to operate)*
The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Contractor System
An information system processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a Contractor in non-GSA facilities.

Deviation
A departure from a security configuration setting required within a GSA hardening guide or from a requirement established by GSA's policies or procedural guides.

General Support System (GSS) or System* (see Major Information System)
An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Federal Information Security Modernization Act of 2014
The FISMA of 2014 provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA recognizes the highly networked nature of the Federal computing environment and is intended to provide effective government wide management and oversight of information security risks. The federal regulation requires an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General (GAO). Requiring Agency reports to include: (1) a description of each major security incident/sets of incidents; (2) total number of information security incidents; (3) a description of each major information security incident

involving the breach of personally identifiable information; (4) any other information specified in annual reporting requirements.

Federal System
An information system processing or containing GSA or Federal data where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor

Note: Any Major Information System having a mix of Federal and Contractor subsystems will be considered a Federal system.

Information Security*
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information System*
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology (IT)*
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which— 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Major Application* (see Major Information System)
An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

> **Note:** All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by the security of the systems in which they operate.

Major Information System (this term replaces General Support System and Major Application)
A system that is part of an investment that requires special management attention as defined in OMB guidance and agency policies, a “major automated information system” as defined in 10

U.S.C. § 2445, or a system that is part of a major acquisition as defined in Supplement to Part 7 of OMB Circular A-11, Capital Programming Guide.

Plan of Action and Milestones*
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.

Security Controls*
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Service and Staff Office (SSO)
References an agency component as identified on the GSA InSite webpage.

Subsystem
A subsystem is a system/application (other than Salesforce applications) categorized with a FIPS 199 security impact level of Low or Moderate, dependent upon the resources provided by its underlying GSS or MA, with the underlying GSS or MA providing the majority of the subsystem's security controls. The supporting GSS or MA must be shown to provide a foundational level of protection for the subsystem; the subsystem may have a FIPS 199 level equal to or below the level of the host GSS or MA.