Plan of Action and Milestones (POA&M) Training Session

Jamie Nicholson
IM-31, Policy, Guidance, & Planning Division
U.S. Department of Energy
Office of the Associate CIO for Cyber Security

Objectives

- **Provide guidance for developing effective POA&Ms.**
- **Discuss partnership role of the OCIO.**
- **Improve understanding of the difference between program and system level POA&M.**
- **Review exercise that demonstrates the possible types of POA&Ms, as well as review documentation requirements.**
- **Provide open forum for discussion.**

What is a POA&M?

- *Plan of Actions and Milestones*

  - A POA&M is a *management tool* for *tracking* the *mitigation* of cyber security *program* and *system level findings/weaknesses.*

Sources of POA&Ms

- *Where do POA&Ms come from?*
  - External findings (e.g., HSS, IG, GAO, Site Office reviews, etc.)
  - Internal findings (e.g., In-house self-assessments, peer reviews, etc.)
  - Certification & Accreditation (C&A) Activities (e.g., Failed certification tests, etc.)

What is not a POA&M?

- *A POA&M is not an Action Tracking Plan.*
- *A POA&M is not a Corrective Action Plan, or CAP.*
  - ➢CAP provides specific information as to remediation of findings/weaknesses.
  - ➢CAP includes a determination of causal factors and trends.

Corrective Action Plan, or CAP

- CAPs are required for all POA&Ms with corrective actions that require more than one (1) year to complete.

- At a minimum, CAPS must include:
  - Root cause analysis
  - Mitigation/resolution alternatives and associated risk analyses
  - Recurrence prevention strategies

- CAPs for findings identified by HSS must comply with guidance established/directed by that organization.
  - DOE O 470.2B, *Independent Oversight and Performance Assurance Program*

Drivers

- *FISMA, Title III, Information Security*
- *OMB M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones*
- *DOE 205.1A, Department of Energy Cyber Security Management*
- *DOE M 205.1-5, Cyber Security Process Requirements Manual*
- *Senior DOE Management PCSPs*

Business Purpose

- *Effective Data Analysis – Consistent, aggregated information is an effective management tool.*
  - Showcase systematic successes and problems.
  - Snapshot of program and system level status.
  - Assists with timely resolution of findings and prioritization of resources.
  - Enhance C&A efforts.

- *POA&M information impacts internal and congressional scorecards.*

- *OMB requires Federal agencies to report all system and program deficiency information quarterly*.

Partnership

- ***OCIO is a partner in the POA&M process*.**

  - We view our office as a resource to assist with issues or questions.

  - We are open to suggestions. You are welcome to contact the OCIO directly if you have suggestions or questions, but please coordinate communications with your POC.

  - You can benefit from information that we have learned as a result of *partnering* with other organizations internal and external to DOE.

Baseline Requirements

- *A POA&M must be developed for each program and system level finding/weakness as identified by:*
  - Office of Health, Safety, and Security (HSS)
  - General Accounting Office (GAO)
  - Office of Inspector General (IG)
  - Internal program and system reviews/self-assessments
  - C&A Activities

Baseline Requirements

- Each POA&M and its associated milestone(s) must have a scheduled completion date that reflects a *reasonable* time period for completion of a remediation activity. ***Findings/weaknesses identified by the GAO and IG are generally expected to be completed within 1 year. Reference DOE O 224.3, Audit Resolution and Follow-up Program.***

- ***Per OMB,*** changes cannot be made to the *original* description of the finding/weakness, milestones, scheduled completion dates, or source. ***Exception to the rule does exist***.

- Reported closure of the finding/weakness and/or milestones must be validated by independent party – not the individual(s) directly responsible for the closure.

Baseline Requirements

- *The following information must be reported on the POA&M when a finding/weakness and/or milestone is completed*:
  - Name and title of individual performing verification
  - Date of verification
- *All completed milestones must be verified by an independent before weakness closure.*
- *All completed findings/weaknesses must remain on POA&M report for a period of 1 year from the date of verification*.

Exception to the Rule

- *Changes cannot be made to original POA&M content unless*:
  - **Changes are fully supported by documentation as required by the originating source (i.e., internal or external) of the finding/weakness.** Changes must be coordinated with your specific Data Call POC.
  - Detail of any changes must be noted in Comment column.

Program vs. System Level

- ***Program Level POA&M***

  - A program level finding/weakness addresses identified cyber security weaknesses or deficiencies that impact the entire cyber security program.

  - For example,
    - Lack of effective password policy across all platforms.
    - Lack of formalized risk assessment process.
    - Lack of approved PCSP

Program vs. System Level

- ***System Level POA&M***

  - A system level finding/weakness addresses an identified weakness associated with an information system with a defined accreditation boundary or a single System Security Plan (SSP).

  - For example,
    - System X does not comply with stated password characteristic requirements.
    - No formal risk assessment documentation exists for System X.
    - System X does not have a required contingency plan

Answers to Common Questions

- POA&Ms are required for findings/weaknesses associated with unclassified and classified systems operated by DOE or DOE contractors.
- System level and program level findings/weaknesses must be documented and divided into two (2) separate templates.
- All applicable cells in the POA&M template for findings/ weaknesses must be completed.
- All findings/weaknesses must be associated with at least one milestone.

Answers to Common Questions

- All findings/weaknesses and milestones must have a Scheduled Completion Date; TBD is not acceptable. Utilize comment field if there is additional information concerning the completion date.
- The Scheduled Completion Date must provide adequate time for verification activities.
- Columns on the standard POA&M template cannot be changed or deleted.

Answers to Common Questions

- Organization can add columns to the RIGHT of the standard template.
- All POA&M data call submissions are to be considered OUO and must be encrypted. *Do not send POA&M data call responses to Cyber Security Mailbox.*
- If the organization does not have any program or system level POA&Ms, then report this status as directed.
- Cyber Security Reporting Dates:
  - 8/01/XXXX – 10/31/XXXX
  - 11/01/XXXX – 1/31/XXXX
  - 2/1/XXXX – 4/30/XXXX
  - 5/1/XXXX – 7/31/XXXX

Answers to Common Questions

- POA&M information must be consistent with information submitted in quarterly Cyber Security Internal Report Cards and Information Security (Metrics) Data Calls.

  - Examples include:
    - Number of findings/weaknesses reported on the Report Card must be consistent with the number of findings/weaknesses reported on the POA&M.
    - Number of operational systems needing C&A and/or certification testing as reported on the Information Security data call must be represented by one or more POA&Ms.
    - Number of findings/weaknesses over 90 days as reported on the Information Security data call must be consistent with POA&M information.
    - Number of findings/weaknesses not completed as scheduled and reported on the Report Card must be consistent with POA&M information.

POA&Ms for Classified Findings/ Weaknesses

- **Do not** submit POA&Ms with classified information.
- **Do not** document the system name, finding/weakness description, weakness category, or milestone descriptions. ***"See Report" must be entered in these fields.***
- ***Do notate the following information:***
  - Classification Level
  - Identified Source
  - Audit Report Number
  - Exhibit 300 or 53 information
  - Site Location and POC Name
  - Resources Required
  - Milestone Number
  - Scheduled and Actual Completion Dates

Hands-On Exercise

Program Review/Self Assessment

Assessment Objective: *Determine if 100% of remote access connections that access SUI/PII utilize 2-factor authentication where one of the factors is provided by a physical device separate from the computer gaining access.*

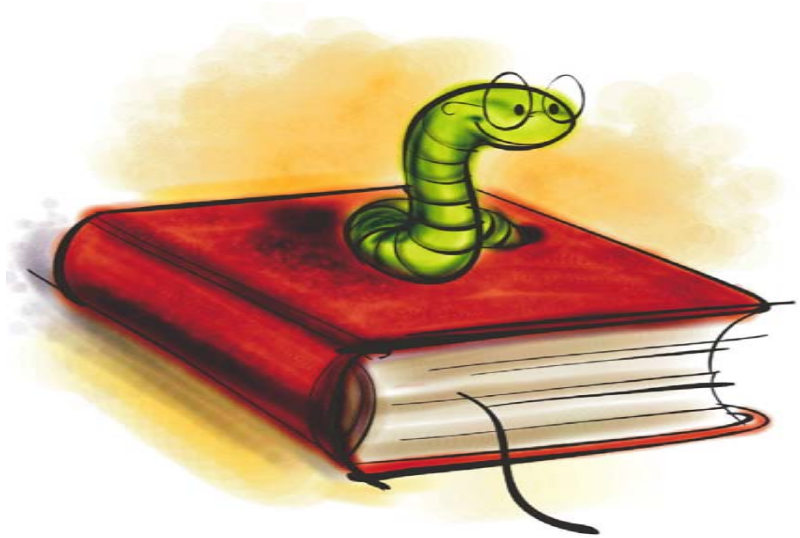
Assessment Method: *Interview and Examine.*

Expected Outcome: *All remote connections (100%) accessing SUI/PII must successfully authenticate to the system using 2-factor authentication before access to such information is granted.*

Actual Result: *Only 45% of remote connections accessing SUI/PII are using 2-factor authentication.*

Evaluation: *Fail.*

Questions ?



Jamie Nicholson

Jamie.nicholson@hq.doe.gov

301-525-2788

Or

Danica Wheelock

Danica.wheelock@hq.doe.gov

202-586-2150