U.S. DEPARTMENT OF ENERGY

Office of the Chief Information Officer

POA&M Training Reference Material



April 2011

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.)

- *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*

Suggested Content of CAP

- A brief overview and summary of the identified weakness/finding.
- Root cause analysis addressing any systematic program weaknesses.
- Description of mitigation/resolution strategies.
- Office or organization responsible for remediation.
- Resource requirements and expected costs.
- Scheduled start and completion date.
- At least one major milestone and completion date.
- Statement of risk assessment, acceptance, and approval.
- Statement of verification requirements to include responsible individual or office and documentation requirements.

- *FISMA, Title III, Information Security*
- *OMB M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones*
- *DOE O 205.1B, Department Cyber Security Management*
- *Senior DOE Management PCSPs (if applicable)*

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*.

- ***OCIO is a partner in the POA&M process.***
  - The OCIO is a resource to assist with issues or questions.
  - The OCIO is 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 the OCIO has 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; see page 8.***
- 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

Color Coding Opportunities

- ***Reporting organizations must follow color coding requirements.***
  - Additions and strikeouts for current reporting quarter must be documented in ***RED***.
  - Verified and completed POA&Ms must be documented in ***BLUE*** if marked for deletion during the current reporting quarter.
  - Transfer of POA&M entry to program-level from system-level (or vice versa) must be documented in ***GREEN*** on both templates.
  - Additions, strikeouts, and transfers must be described in comment column.

Program-Level POA&M Template FY2011 2nd Quarter

Weakness Data

Weakness CIO Reference Number	Classified Weakness? Yes or No	Identified Source	Audit Report Number	DARTS Finding Number	DARTS Recommendation Number	Site Location	Weakness POC Name (Format: Last Name, First Name)

1. ***Weakness CIO Reference Number -*** This reference number will be assigned by DOE's Office of Cyber Security; do not change this number.

2. ***Classified Weakness? (Yes or No) -*** Indicate Classified or Unclassified. If classified, enter **SEE REPORT** in the appropriate cells.

3. ***Identified Source –*** Indicate the actual source of the weakness. For example, IG/GAO/HSS audit, self assessment, C&A, etc.

4. ***Audit Report Number -*** Enter the audit report number assigned by the organization/entity that cited the weakness for the Program or Field Office. For example, DOE/IG-0491, GAO-05-597R, HSS, etc.

5. ***DARTS Finding Number -*** See the DARTS Report for the finding number. If the finding is not required to be listed in DARTS, enter **N/A** in this cell.

6. ***DARTS Recommendation Number*** - See the DARTS Report for the recommendation number. If the finding is not required to be listed in DARTS, enter **N/A** in this cell.

7. ***Site Location -*** Enter the site/location responsible for the weakness.

8. ***Weakness POC Name (Required Format: Last Name, First Name) -*** This is the name of the primary point of contact (POC) for the weakness. For Science POA&Ms, an accountable person such as the ISSO or ISSM must be listed.

Program-Level POA&M Template FY2011 2nd Quarter

Weakness Data

Weakness POC Title	Significant Deficiency Yes or No	Weakness Category	Weakness Description	Weakness Resources Required	Weakness Start Date MM/DD/YYYY

9. ***Weakness POC Title -*** This is the title (i.e., ISSO, System Owner, etc. as designated) of the individual who is the primary contact for the system.

10. ***Significant Deficiency (Yes or No) -*** This is defined as a weakness in an agency's overall information system security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. The risk presented by such a weakness is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. A ***significant deficiency*** under FISMA is to be reported as a material weakness under the Federal Managers Financial Integrity Act (FMFIA). ***NOTE: if the response is YES, enter SEE REPORT in the Classified Weakness field.***

11. ***Weakness Category -*** Indicate the control family that the weakness is associated with. Use one of the following**.**

1. Access Control	2. Awareness and Training	3. Audit and Accountability	4. Certification, Accreditation, and Security Assessments	5. Configuration Management
6. Contingency Planning	7. Identification and Authentication	8. Incident Response	9. Maintenance	10. Media
11. Physical and Environmental Protection	12. Planning	13. Personnel Security	14. Risk Assessment	15. System and Service Acquisition
16. System and Communications Protection	17. System and Information Integrity	18. Policy	19. Other	

Program-Level POA&M Template FY2011 2nd Quarter

Weakness Data

12. ***Weakness Description -*** This is a statement or brief description for a particular weakness. Sensitive descriptions are not necessary, but sufficient data must be provided to permit oversight and tracking. ***Note: Any change to the Weakness Description requires a new entry. The Weakness must be superseded with a new entry.***

13. ***Weakness Resources Required -*** This is the estimated monetary amount required to mitigate a weakness. At least $1 amount is required except for Bonneville Power Administration (BPA)***. Note: This cost should be fully burdened.***

14. ***Weakness Start Date (Required Format - MM/DD/YYYY) -*** This is the date that the entry was established as a weakness***.***

Program-Level POA&M Template FY2011 2nd Quarter

Weakness Data

Weakness Scheduled Completion Date MM/DD/YYYY	Weakness Status	Weakness Actual Completion Date MM/DD/YYYY

15. ***Weakness Scheduled Completion Date (Required Format - MM/DD/YYYY) -*** This is the date that the weakness is scheduled to be completed**.**

16. ***Weakness Status -*** Indicate Ongoing, Superseded, or Ongoing. ***Note: Superseded must be fully explained in the Changes to Milestone or Current Status field.***

17. ***Weakness Actual Completion Date (Required Format - MM/DD/YYYY) -*** This is the actual date that the weakness is completed***.*** ***Note: All Milestones must be verified before the Weakness can be completed.***

Program-Level POA&M Template FY2011 2nd Quarter

Milestone Data

Milestone Number	Milestone Description	Milestone Scheduled Completion Date MM/DD/YYYY	Changes to Milestone or Current Status	Milestone Status	Name of Person Verifying Milestone Completion (Format: Last Name, First Name)

1. ***Milestone Number -*** This is a sequential number associated with a milestone and is assigned by the organization. A weakness can have several milestones. ***Note: Zero can be used as a summary milestone; it will not be included in the milestone counts***.

2. ***Milestone Description -*** This is the brief description of the milestone***.***

   Example of a description for a summary milestone #0:
   Project will correct weakness: XXX,
   By implementing the following action(s): xxx.
   This was identified by or in: xxx.
   The POA&M reference number is XXX.

3. ***Milestone Scheduled Completion Date (Required Format MM/DD/YYYY) -*** This is the date the milestone is scheduled to be completed.

4. ***Changes to Milestone or Current Status –*** Required text that describes changes to a milestone.

5. ***Milestone Status –*** Indicate Ongoing, Superseded, Pending Verification, or Completed.

6. ***Name of Person Verifying Milestone Completion (Required Format – Last Name, First Name) -*** This is an authorized person, other than the person directly responsible for mitigating the weakness, who is verifying that the milestone is completed***.***
   Note: For Science, the person verifying that the milestone is closed is the cognizant AO or AODR.

Program-Level POA&M Template FY2011 2nd Quarter

Milestone Data

Title of Person Verifying Milestone Completion	Milestone Date of Verification MM/DD/YYYY	Milestone Actual Completion Date MM/DD/YYYY

7. **Title of Person Verifying Milestone Completion -** This is the title of the person who is verifying that the milestone is completed.

8. **Milestone Date of Verification (Format Required – MM/DD/YYYY) -** This is the date that the verification is completed**.** ***Note: The actual completion date of the milestone cannot precede the date of verification.***

9. **Milestone Actual Completion Date (Format Required – MM/DD/YYYY) -** This is the actual date the milestone is completed**.**

Program-Level POA&M Template FY2011 2nd Quarter

Row Data

Program/Field/Staff Office Comments	DOE OCIO Review Comments

1. **Program/Field/Staff Office Comments -** This field is for the Program, Field, or Staff offices to enter any necessary comments pertaining to the weakness or milestone in this row**.**

2. **DOE OCIO Review Comments -** This field captures the DOE OCIO reviewer comments pertaining to the highlighted cell(s) in this row that need to be addressed by the Program/Field//Staff Office prior to the next reporting period.

System-Level POA&M Template FY2011 2nd Quarter

Weakness Data

Weakness CIO Reference Number	System Name for this Weakness	NSS Yes or No	System Impact Level	Identified Source	Audit Report Number	DARTS Finding Number	DARTS Recommendation Number	Exhibit 300 or 53 Unique Project ID

1. **Weakness CIO Reference Number -** This reference number will be assigned by DOE's Office of Cyber Security; do not change this number**.**

2. **System Name for this Weakness -** Enter the system name that is associated with the weakness**.** ***Note: For classified systems, use the pseudonym (e.g., alias or common acronym) for the system.***

3. **NSS (Yes or No) –** Indicate Yes or No for National Security System (NSS).

4. **System Impact Level -** Enter the appropriate system impact level of High, Moderate, or Low**.**

5. **Identified Source –** Indicate the actual source of the weakness. For example, IG/GAO/HSS audit, self assessment, C&A, etc.

6. **Audit Report Number -** Enter the audit report number assigned by the organization/entity that cited the weakness for the Program or Field Office. For example, DOE/IG-0491, GAO-05-597R, HSS, etc.

7. **DARTS Finding Number -** See the DARTS Report for the finding number. If the finding is not required to be listed in DARTS, enter **N/A** in this cell.

8. **DARTS Recommendation Number -** See the DARTS Report for the recommendation number**.** If the finding is not required to be listed in DARTS, enter **N/A** in this cell.

9. **Exhibit 300 or 53 Unique Project ID -** This unique identifier links the POA&M to the Exhibit 300 or Exhibit 53.

System-Level POA&M Template FY2011 2nd Quarter

Weakness Data

Exhibit 300 or 53 Project Name	Exhibit 300 or 53 Security Cost	Site Location	Weakness POC Name (Format: Last Name, First Name)	Weakness POC Title	Significant Deficiency Yes or No	Weakness Category	Weakness Description

10. **Exhibit 300 or 53 Project Name - Project** name that aligns the POA&M to the Exhibit 300 or 53 investment name.

11. **Exhibit 300 or 53 Security Cost -** This figure should reflect the investment's total security cost budgeted for Cyber Security on an annual basis.

12. **Site Location -** Enter the site/location responsible for the weakness.

13. **Weakness POC Name (Required Format – Last Name, First Name) -** This is the name of the primary point of contact (POC) for the weakness. For Science POA&Ms, an accountable person such as the ISSO or ISSM must be listed.

14. **Weakness POC Title -** This is the title (i.e., ISSO, System Owner, etc. as designated) of the individual who is the primary contact for the system.

15. **Significant Deficiency (Yes or No) -** This is defined as a weakness in an agency's overall information system security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. The risk presented by such a weakness is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. A ***significant deficiency*** under FISMA is to be reported as a material weakness under the Federal Managers Financial Integrity Act (FMFIA). ***NOTE: if the response is YES, enter SEE REPORT in the NSS Yes or No field.***

16. **Weakness Category -** Indicate the control family that the weakness is associated with. Refer to the Control Family table on page 12 of this handbook.

17. **Weakness Description -** This is a statement or brief description for a particular weakness. Sensitive descriptions are not necessary, but sufficient data must be provided to permit oversight and tracking. ***Note: Any change to the Weakness Description requires a new entry. The Weakness must be superseded with a new entry.***

System-Level POA&M Template FY2011 2nd Quarter

Weakness Data

Weakness Resources Required	Weakness Start Date MM/DD/YYYY	Weakness Scheduled Completion Date MM/DD/YYYY	Weakness Status	Weakness Actual Completion Date MM/DD/YYYY

18. **Weakness Resources Required -** This is the estimated monetary amount required to mitigate a weakness. At least $1 amount is required except for Bonneville Power Administration (BPA). ***Note: This cost should be fully burdened.***

19. **Weakness Start Date (Required Format – MM/DD/YYYY) -** This is the date that the entry was established as a weakness.

20. **Weakness Scheduled Completion Date (Required Format – MM/DD/YYYY) -** This is the date that the weakness is scheduled to be completed.

21. **Weakness Status -** Indicate Ongoing, Superseded, or Ongoing. ***Note: Superseded must be fully explained in the Changes to Milestone or Current Status field.***

22. **Weakness Actual Completion Date (Required Format – MM/DD/YYYY) -** This is the actual date that the weakness is completed. ***Note: All Milestones must be verified before the Weakness can be completed.***

System-Level POA&M Template FY2011 2nd Quarter

Milestone Data

Milestone Number	Milestone Description	Milestone Scheduled Completion Date MM/DD/YYYY	Changes to Milestone or Current Status	Milestone Status	Name of Person Verifying Milestone Completion (Format: Last Name, First Name)	Title of Person Verifying Milestone Completion

1. **Milestone Number -** This is a sequential number associated with a milestone and is assigned by the organization. A weakness can have several milestones. ***Note: Zero can be used as a summary milestone; it will not be included in the milestone counts.***

2. **Milestone Description -** This is the brief description of the milestone. See page 15 of the handbook for an example of a summary milestone.

3. **Milestone Scheduled Completion Date (Required Format – MM/DD/YYYY) -** This is the date the milestone is scheduled to be completed.

4. **Changes to Milestone or Current Status -** Required text that describes changes to a milestone.

5. **Milestone Status -** Indicate Ongoing, Superseded, Pending Verification, or Completed.

10. **Name of Person Verifying Milestone Completion (Required Format – Last Name, First Name) -** This is an authorized person, other than the person directly responsible for mitigating the weakness, who is verifying that the milestone is completed***.***
Note: For Science, the person verifying that the milestone is closed is the cognizant AO or AODR.

6. **Title of Person Verifying Milestone Completion -** This is the title of the person who is verifying that the milestone is completed.

System-Level POA&M Template FY2011 2nd Quarter

Milestone Data

Milestone Date of Verification MM/DD/YYYY	Milestone Actual Completion Date MM/DD/YYYY

7. **Milestone Date of Verification (Required Format – MM/DD/YYYY) -** This is the date that the verification is completed**.** ***Note: The actual completion date of the milestone cannot precede the date of verification.***

8. **Milestone Actual Completion Date (Required Format – MM/DD/YYYY) -** This is the actual date the milestone is completed.

System-Level POA&M Template FY2011 2nd Quarter
Row Data

Program/Field/Staff Office Comments	DOE OCIO Review Comments

1. **Program/Field/Staff Office Comments -** This field is for the Program, Field, or Staff offices to enter any necessary comments pertaining to the weakness or milestone in this row.

2. **DOE OCIO Review Comments -** This field captures the DOE OCIO reviewer comments pertaining to the highlighted cell(s) in this row that need to be addressed by the Program/Field//Staff Office prior to the next reporting period.