POA&M Verification & Validation (V&V) Training

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

Ground Rules

- *Please ask questions at any time.*
- *Ideas/suggestions? Please utilize 'feet' sticky notes for parking lot issues.*
- *Presentation addresses OCIO V&V process. Program-specific requirements are not covered.*
- *TAF specifics will not be discussed.*

Objectives

- *Discuss benefits of performing verification and validation procedures.*
- *Provide direction on how to effectively verify and validate POA&M information.*
- *Review examples that demonstrate color coding as a method for identifying change, issues, or questions.*
- *Provide open forum for discussion.*

Regulatory Drivers

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

Lessons Learned

- *POA&M information submitted in the past has not been consistent.*

- *Why is this an issue?*
  - *Incorrect information distorts true picture of asset protection within the Department.*
  - *Difficult or impossible to do value-added analysis of information.*

The Dawning of V&V

- *OCIO recognized the need for better communication to program/staff office POCs.*
  - *Developed improved templates*
  - *Offered data call conference calls to discuss expectations*
  - *Provided individual training*
- *Began aggressive effort to perform line-by-line review of all POA&M information.*
- *As a result, consistent deficiencies were documented and identified.*

Benefit to DOE

- *Consistent information for aggregation.*
- *Clear and sound picture of Department's security posture.*
- *Ensure deficiencies are resolved in timely manner.*
- *Improved communication.*

Partnership

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

Rules of the Road
Color Coding Requirements

- Additions and strikeouts for current reporting quarter must be document in *RED* font.
- Verified and completed POA&Ms must be highlighted 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.

Rules of the Road

1. Identify missing, incorrect or incomplete information. The OCIO highlights this information in YELLOW.

   - If an entire column is missing, the column is highlighted.
   - If an entire row is missing, the row is highlighted.

Weakness Status	Milestone Number	Milestone Description	Milestone Scheduled Completion Date MM/DD/YY YY	Milestone Actual Completion Date MM/DD/YY YY
Ongoing		Identify remaining remote connections that have not implemented 2-factor authentication.	6/30/2008	6/20/2008
		Purchase required number of RSA tokens.	10/31/2008	

Rules of the Road

2. Identify overdue information. The OCIO highlights this information in PINK.

Milestone Number	Milestone Description	Milestone Scheduled Completion Date MM/DD/YYYY	Milestone Actual Completion Date MM/DD/YYYY	Changes to Milestone or Current Status	Milestone Status	Name and Title of Person Verifying Milestone Completion	Milestone Date of Verification MM/DD/YYYY
1	Review/update CP	12/15/08	12/01/2008		Completed	D. Wheelock, CSPM	12/01/2008
2	Test CP	1/15/09			Ongoing		
3	Document Results	3/1/09			Ongoing		
4	Finalize Report	3/15/09			Ongoing		

Rules of the Road

3. Identify items that require further research. The OCIO highlights this information in PURPLE.

Weakness Scheduled Completion Date MM/DD/YYYY	Weakness Actual Completion Date MM/DD/YYYY	Weakness Status	Milestone Number	Milestone Description	Milestone Scheduled Completion Date MM/DD/YYYY	Milestone Actual Completion Date MM/DD/YYYY
1/15/2009	1/15/2009	Completed	1	Update annual cyber security training.	12/1/2008	11/15/2008
			2	Distribute training to General users.	12/30/2008	12/20/2008
			3	Complete annual training requirement.	1/15/2009	1/31/2009

Rules of the Road

4. Identify POA&Ms that need to be moved to either the program or system level spreadsheet. This information must be highlighted in GREEN.

Milestone Number	Milestone Description	Milestone Scheduled Completion Date MM/DD/YYYY	Milestone Actual Completion Date MM/DD/YYYY	Changes To Milestone or Current Status	Milestone Status	Name and Title of Person Verifying Milestone Completion
1	Update annual cyber security training.	4/1/2009		Has been determined that finding was incorrectly assigned program-level POA&M. Deficient training is system-specific; site is not deficient on annual training requirement.	Ongoing	
2	Distribute training to General users.	5/1/2009			Ongoing	
3	Complete annual training requirement.	6/30/2009			Ongoing	

Rules of the Road

5. Identify items that should be marked for deletion. This information must be highlighted in BLUE.

Weakness Scheduled Completion Date MM/DD/YYYY	Weakness Actual Completion Date MM/DD/YYYY	Weakness Status	Milestone Number	Milestone Description	Milestone Scheduled Completion Date MM/DD/YYYY	Milestone Actual Completion Date MM/DD/YYYY
1/31/2008	1/31/2008	Completed	1	Update annual cyber security training.	11/1/2007	10/15/2007
			2	Distribute training to General users.	12/1/2007	12/1/207
			3	Complete annual training requirement.	1/31/2008	1/31/2008

Rules of the Road

6. Documents to be used during V&V

   - *System-level POA&M Report*
   - *Program – level POA&M Report*
   - *Information Security Report (ISR) – formerly known as Metrics*

V&V Tasks/Priority #1

1. Verify that all cells that require data are completed properly.

    1) *If no CIO Number, indicates new entry and text is RED for entire row.*
    2) *For completed milestones ensure that name, title, and date have been entered.*
    3) *Verify that all weakness and milestones have a scheduled completion date.*
    4) *Verify that dates are in **MM/DD/YYYY** format.*
    5) *Validate that the 'Weakness Status' is properly completed; if closed, all milestones must be verified closed and the 'Milestone Status' indicates 'Complete.'*
    6) *Verify that 'Resources Required' is dollar amount; TBD or $0 is not acceptable.*

V&V Tasks/Priority #1

2. Verify correctness of milestone completion dates.

    1) *Verify that 'Milestone Dates of Verification' are on or before the 'Milestone Actual Completion Dates' associated with a weakness.*

    2) *Verify that milestones with a status of 'Pending Verification' do not have a 'Milestone Actual Completion Date.'*

V&V Tasks/Priority #1

3. Verify correctness of weakness completion dates.

    1) *Verify that 'Weakness Actual Completion Date' and/or the 'Milestone Actual Completion Dates' are NOT beyond (later than) the last day of the current reporting period.*

    2) *Verify that all 'Milestone Actual Completion Dates' are the same date or earlier than the 'Weakness Actual Completion Date.'*

V&V Tasks/Priority #1

4. **For system-level POA&Ms only**, reconcile data for systems being reported as having an IATO.

   1) *Verify that systems listed in the Information Security Report (ISR) as having an IATO are also listed in the system-level POA&M with a designated 'Weakness' Category' of Certification, Accreditation, and Security Assessments.*

Program Office/Site	System Name Having an IATO	System Impact Level	Exhibit 53 Unique Project Identifier (UPI)

   2) *If not, notify the originating program office or site. Note: In this case, the OCIO would highlight this ISR entry in PURPLE indicating further research needed.*

V&V Tasks/Priority #1

5. **For system-level POA&Ms only**, reconcile data reported in the Information Security Report (ISR) as 'Non C&A Report' with data reported in the system-level POA&M.

   1) *Verify that systems listed in the ISR on the 'Non C&A Report' are also listed in the system-level POA&M with a designated 'Weakness' Category' of Certification, Accreditation, and Security Assessments.*

Program Office/Site	System Name Not C&A'd	System Impact Level	Exhibit 53 Unique Project Identifier (UPI)

   2) *If not, notify the originating program office or site. Note: The OCIO would highlight this ISR in PURPLE indicating further research needed.*

V&V Tasks/Priority #1

6. For both system-level and program-level POA&Ms:

a) Identify the number of ongoing weaknesses at the end of the reporting period that are:

1) 1 to 89 days overdue from the 'Weakness Scheduled Completion Date'

2) 90 to 120 days overdue from the 'Weakness Scheduled Completion Date'

3) Over 120 days overdue from the 'Weakness Scheduled Completion Date'

V&V Tasks/Priority #1

6. For both system-level and program-level POA&Ms:

b) Tabulate and document the following:

1) Total number of weaknesses.

2) Total number of new weaknesses.

3) Total number of ongoing weaknesses.

4) Total number of ongoing overdue weaknesses using data collected in 6a.

Note: Program offices have access to the OCIO-developed worksheet used for tracking information in 6a and 6b.

V&V Tasks/Priority #1

7. **For system-level POA&Ms only**, verify the *number of systems* with overdue weaknesses in the Information Security Report (ISR) at the end of the reporting period against overdue information identified in step 6a as follows:

    1) *1 to 89 days overdue from the 'Weakness Scheduled Completion Date'*

    2) *90 to 120 days overdue from the 'Weakness Scheduled Completion Date'*

    3) *Over 120 days overdue from the 'Weakness Scheduled Completion Date'*

Ultimate Goal - Success

- *Consistent, accurate information is our ultimate goal.*
- *Accurate depiction of program management; enhances situational awareness.*
- *Showcases areas of success and areas needing improvement.*

Questions ?