

**U.S. Department of Energy
Cyber Security Program**

**PLAN OF ACTION AND MILESTONES
GUIDANCE**



September 2006

***This Guidance document was
developed and issued outside of the
Departmental Directives Program.***

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance applies Office of Management and Budget (OMB) Memorandum (M)-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, annual OMB FISMA reporting instructions, and other applicable Departmental and Federal information technology security requirements and regulations.

The Plan of Actions and Milestones (POA&M) process is a management tool for tracking the mitigation of cyber security program and system-level weaknesses. The intent of the POA&M is threefold: (1) to be a management tool to assist agencies in closing their security gaps; (2) assist Inspectors General in their evaluation work of agency security performance; and (3) assist OMB with oversight responsibilities.

POA&Ms assist decision-makers in identifying, assessing, prioritizing, and monitoring corrective efforts for these weaknesses across their organization. This Guidance provides a unified and consistent approach to the POA&M process to be addressed in Program Cyber Security Plans (PCSPs).

The DOE Office of the Chief Information Officer (OCIO) will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. CANCELLATIONS.

None.

3. APPLICABILITY.

- a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to Which DOE CIO Guidance CS-6 is Applicable*.

Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units and for ensuring that those requirements are incorporated into contracts.

- b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and

practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.

- c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.
- d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPO)*; the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

4. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its issuance. If Senior DOE Management cannot address all of the criteria by that date, Senior DOE Management is to establish a POA&M for implementation of this Guidance into their PCSPs.

5. CRITERIA.

- a. Senior DOE Management is responsible for developing, documenting and implementing a POA&M management process for all operating units, programs, and systems covered under the organization's PCSP. The documentation is to include processes to:
 - (1) Review and verify accuracy and comprehensiveness of POA&M reporting for each operating unit/program/system to include the following.
 - (a) Reporting of all program and system-level findings identified by the Office of Performance Assessment and Oversight, General Accounting

Office, Office of Inspector General, findings from the Financial Audit, and any open action items resulting from internal security reviews

- (b) Identification of program and system-level security POA&Ms for all systems with open corrective actions.
 - (c) Validation of all negative reports.
 - (d) Appropriate identification and documentation of POA&Ms for National Security Systems
 - (e) Verification, validation, and documentation for closure of each POA&M milestone
- (2) Integrate POA&M identification, tracking, and review requirements in self-assessment, certification and accreditation, and contingency planning policies of the PCSP.
 - (3) Review and assess POA&M activities for each operating unit/program/system on at least a quarterly basis.
 - (4) Report to the Office of the Chief Information Officer in accordance with the Department's FISMA reporting requirements.
- b. Program Cyber Security Plan. Senior DOE Management PCSPs are to be consistent with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE Manual 205.1-X, *National Security Systems Controls*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement POA&M policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs.
- (1) **Corrective Action Plans**. The development of corrective action plans for remediation of identified cyber security weaknesses, vulnerabilities, and findings is a key element of the POA&M process. DOE Directives require corrective action plans for cyber security-related findings identified by the Inspector General and the Office of Security and Safety Performance Assurance. Senior DOE Management PCSPs can require preparation of corrective action plans for other weaknesses based on the organization's mission, environment, and specific needs. Not all items that will be tracked in POA&Ms are required to have corresponding corrective action plans. Senior DOE Management PCSPs are to ensure that operating units define, document, and implement corrective action plan processes that include the following.

- (a) Standard report content.
 - i. A brief overview and summary of the identified weakness, vulnerability, or finding
 - ii. Root cause analysis addressing any systemic program weaknesses
 - iii. Mitigation/resolution and recurrence prevention strategies
 - iv. Office or organization responsible for remediation
 - v. Resource requirements and expected cost
 - vi. Scheduled start and completion date
 - vii. At least one major milestone and completion date
 - (b) Risk assessment and acceptance, approval, and communication procedures
 - (c) Update procedures to include tracking and documenting of implementation status for each milestone (in accordance with DOE Directives if applicable).
 - (d) Verification procedures (including independent validation) and documentation for the closure of each milestone.
- (2) POA&Ms. In accordance with FISMA reporting requirements, all cyber security weaknesses requiring corrective action are to be incorporated into the POA&M process, whether or not a corrective action plan has been prepared. The lack of self-assessments, risk assessments, security plans, certification and accreditation, contingency plans, and implementation of other requirements (including the PCSP) must be included. Senior DOE Management PCSPs are to require operating units to:
- (a) Develop, implement, and manage POA&Ms for their cyber security program (including projects planned as a result of program improvements) and systems they own and operate that have identified security weakness.
 - (b) Track, maintain, review, and prioritize POA&M activities on at least a quarterly basis. The procedure should include a regular review of the POA&Ms and verification that all applicable findings are being tracked. In addition to regularly scheduled reviews, a POA&M assessment is to be completed when there are changes in roles and responsibilities, or new executive, legislative, technical or Departmental guidance is issued; changes in vulnerabilities, risks or threats occur; Interim Authority to

Operate (IATO) exceeds 180 days; and/or new vulnerability findings are identified in an audit, review, or self-assessment.

- (c) Define processes for defining, documenting, and submitting POA&Ms for National Security Systems
- (d) Report to the Senior DOE Management organization on a regular basis (at least quarterly) on their remediation progress. The POA&M update information is included with quarterly information system security metrics to assist in meeting the Department's FISMA reporting requirement. Statistics gathered from the POA&Ms include:
 - i. Total number of weaknesses identified at the start of the quarter.
 - ii. Number of weaknesses for which corrective action was completed on time by the end of the quarter.
 - iii. Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled.
 - iv. Number of weaknesses for which corrective action has been delayed.
 - v. Number of new weaknesses discovered following the last POA&M update and how they were identified.
 - vi. Number of systems with IATO in excess of 90 days.
- (e) Link applicable POA&Ms to budget requests through the business case process required in OMB budget guidance (Circular A-11).

c. POA&M Contents

- (1) Each POA&M must include all program and system-level findings identified by the Office of Performance Assessment and Oversight, General Accounting Office, Office of Inspector General, findings from the annual Financial Audit, and any open action items resulting from internal security reviews.

The lack of self-assessments, risk assessments, security plans, certification and accreditation, contingency plans, and implementation of other requirements are considered weaknesses and must be included in the POA&M.

- (2) A program and system-level security POA&M must be completed for all systems with open corrective actions. A negative report must be provided if there are no findings to report.

- (3) Reported closure of milestones and/or findings must be validated by someone other than the person(s) directly responsible. Whenever a milestone and/or finding is closed, the following information must be provided in the POA&M.
 - Milestone/finding closure validated? (yes or no);
 - Name and position/title of person validating; and
 - Date of verification.
- (4) All findings must be reported unless they have been closed and verified for a period of one (1) year.
- (5) A brief overview and summary of the identified weakness, vulnerability, or finding
- (6) Office or organization responsible for remediation
- (7) Scheduled start and completion date
- (8) At least one major milestone and completion date

6. REFERENCES.

References are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

7. DEFINITIONS.

Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

8. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE
CIO GUIDANCE CS-6 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration