# Plan of Action and Milestones (TMR-6)
**August 10, 2007**

Department of Energy (DOE) Order 205.1A, *Department of Energy Cyber Security Management*, charges Senior DOE Management to implement cyber security within their respective organizations, based on their determination, assessment, and documentation of DOE and program-unique threats and risks. In carrying out this charge, Senior DOE Management is required by the Order to develop a Program Cyber Security Plan (PCSP) that defines cyber security requirements for all subordinate organizations and programs. The Order requires that the PCSP requirements comply with the Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, Office of Management and Budget (OMB) directives, Federal Information Processing Standards (FIPS), Departmental policies, and DOE Chief Information Officer (CIO) Cyber Security Technical and Management Requirements (TMRs). This TMR provides Senior DOE Management general direction and minimum requirements to be used in preparing each PCSP.

The Plan of Action and Milestones (POA&M) process is a management tool for tracking the mitigation of cyber security program and system-level weaknesses. This TMR identifies topics concerning POA&M management that are to be covered in each PCSP, and it provides specific direction applicable to the DOE environment and OMB guidance, enabling Senior DOE Management to implement an organizational approach for the development and management of POA&Ms. It also provides for the Departmental implementation of OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, and annual OMB Federal Information Security Management Act (FISMA) reporting instructions**.** Senior DOE Management may specify and implement additional requirements in each PCSP to address specific risks, vulnerabilities, or threats within its operating units.

## Cancellations

This TMR replaces DOE CIO Guidance CS-6, *Plan of Actions and Milestones*, dated September 2006.

## Implementation

This document defines management and technical cyber security requirements to be incorporated into Senior DOE Management PCSPs within 90 days of the TMR issue date.

## Requirements

### TMR-6-1, Senior DOE Management POA&M Process

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing a POA&M policies and processes for all operating units, programs, and systems to:

1. Link applicable POA&Ms to budget requests through the business case process required in OMB budget guidance (OMB Circular A-11).

2. Integrate requirements for identifying, tracking, and reviewing POA&Ms in self-assessment, certification and accreditation, incident management, capital planning and budgeting, and contingency planning policies of the PCSP.

3. POA&M Reporting. In accordance with the Department's FISMA reporting requirements, Senior DOE Management must report POA&M status for all operating units, programs, and classified and unclassified information systems through the Office of the Chief Information Officer. (Data is gathered by the OCIO from the POA&Ms for Departmental FISMA reporting.) At a minimum, POA&M reporting must include the following.

   a. Program and system-level findings for all classified and unclassified systems, including those identified by the Office of Health, Safety, and Security; General Accounting Office; and Office of Inspector General; findings from the Financial Audit; any weaknesses and open action items resulting from internal program and system reviews; and incidents.

   b. Senior DOE Management is to verify and validate any quarterly reports from operating units that contain no POA&Ms (i.e., no findings from any source to report).

   c. The lack of self-assessments, risk assessments, security plans, privacy impact assessments, certification and accreditation, contingency plans, and implementation of PCSP and other cyber security-related requirements (e.g., requirements in program-specific Directives or contract documents) must be included in the POA&M.

   d. For findings other than those resulting from a Government Accountability Office (GAO) or Inspector General (IG) audit (see DOE O 224.3, *Audit Resolution and Follow-up Program*), the scheduled completion date for each POA&M and milestone must reflect a reasonable time period for completion of the remediation activity.

   e. Reporting on remediation progress must be accomplished in accordance to the Senior DOE Management PCSP but not less frequently than quarterly.

   f. Once the POA&M has been reported, changes are not to be made to the original description of the weakness, key milestones and scheduled completion dates, or source. Notations for any modifications to the original entry are to be made separately and identified as "Changes to Milestones."

   g. Reported closure of milestones and/or findings must be validated by someone other than the person(s) directly responsible for the closure. Whenever a milestone or finding is closed, the following information must be provided in the POA&M.

(1) Date of completion

(2) Validation of Milestone/finding closure

(3) Name and position/title of validator

(4) Date of verification

h. All closed, verified milestones must remain on the report until the finding is closed.

i. All closed, verified findings must remain on the report for a period of 1 year.

j. Verification and validation for closure of each POA&M and milestone must be documented.

k. POA&M reports are to be marked and protected as appropriate; at a minimum, reports are to be considered Official Use Only.

4. POA&M Contents. 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. Each POA&M must contain:

a. A brief overview and summary of the identified weakness (i.e., vulnerability, finding, etc.), written at an unclassified level.

b. Office or organization responsible for remediation.

c. Identification of program or system level issue.

d. Proposed/approved source and amount of resources required, where applicable, for remediation (i.e., funding, personnel, expertise, new system, etc.).

e. For system-level POA&Ms, the unique project identifier and project name from the OMB Exhibit 300 or Exhibit 53, where applicable. For Exhibit 53 systems, security costs must also be included.

f. Citation of source of identification of the weakness.

g. Scheduled completion date

h. At least one major milestone and scheduled completion date

i. Verification and documentation for the closure of each milestone.

5. POA&M Management. POA&M activities for each operating unit/program/system must be reviewed and assessed on at least a quarterly basis. POA&Ms must be reviewed and updated as needed when there are changes in roles and responsibilities; executive, legislative, technical or Departmental guidance; and vulnerabilities, risks

or threats occur; and if new findings are identified in an audit, review, or self-assessment. POA&M update information is included with quarterly information system security metrics to assist in meeting the Department's FISMA reporting requirement.

**TMR-6-2, Corrective Action Planning**

The corrective action plan (CAP) provides specificity regarding remediation that is generally not included in a POA&M, allowing for closer management of the remediation process; determination of causal factors and trends; and assessment of the effectiveness of corrective actions to ensure successful resolution and prevention of the same or similar problems. Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing processes and procedures for the development, implementation, and management of corrective action plans to include the following.

1. The development of corrective action plans for program- and system-level weaknesses identified in self-assessments, reviews, audits, or incidents that are not covered under CAP requirements established by the Office of Health, Safety, and Security (see DOE O 470.2B, Independent Oversight and Performance Assurance Program, DOE O 414.1C, Quality Assurance, and DOE M 470.4-1, Safeguards and Security Program Planning and Management). Corrective Action Plans are recommended for all POA&Ms that require more than 1 year to complete.

2. Standard Corrective Action Plan content, to include root cause analysis addressing any systemic program weaknesses, mitigation/resolution alternatives and associated risk analyses, and recurrence prevention strategies

3. The extent of detail in the CAP should be determined based on the significance, impact, number, and complexity of the problem findings and corrective actions to resolve the findings.

**TMR-6-3, Operating Unit Policies and Procedures**

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement policies and procedures for POA&Ms compliant with the requirements defined in the PCSP and commensurate with the level of security required for the organization's environment and specific needs.