Cyber Security Technical and Management Requirements

Configuration Management (TMR-8)
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 document provides Senior DOE Management general direction and minimum requirements to be used in preparing each PCSP.

Configuration Management (CM) applies administration, technical direction, and surveillance to identify and document functional and physical characteristics of a configuration item, control changes, record and report change processing and implementation, and verify compliance with specified requirements. This TMR establishes a risk-based CM approach that is to be covered in each PCSP for information systems within the DOE. It also provides for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-70, *Security Configuration Checklists Program for IT Products—Guidance for Checklist Users and Developers*, and addresses minimum security requirements for Windows XP and Vista as defined in the OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.* 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-8, *Configuration Management Guidance*, dated November 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-8-1, Senior DOE Management Configuration Management Program
Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing configuration management policies and processes for all operating units, programs, and systems. The Senior DOE Management PCSP is to describe the configuration management process to include the following.

1. Configuration Management documentation, including System Security Plans (SSPs), Contingency Plans, user and administrator guidance, system component inventory, Configuration Management Plan (CMP), and Security Testing and Evaluation (ST&E) procedures.

2. Identification of the roles and responsibilities for change approval/disapproval to establish a new baseline

3. Policy and processes for security configuration management for each information system for configuration documentation, change control and tracking, and approval of configuration changes to all National Security Systems and other information systems in Security Categories Moderate and High to include at least the following.
   a. Information system and configuration item unique identification and labeling
   b. Design documentation, including system specification and configuration item specification(s)
   c. Configuration change identification, tracking, control, and history
   d. Configuration status accounting to track changes from identification to implementation to produce a new baseline
   e. Security configuration checklist for operating system software, application software, and hardware platforms
   f. Configuration auditing to trace modifications to configuration items for authorized changes
   g. Integration of vulnerability and patch management processes
   h. Documentation of configuration change control methodology and tools used
   i. Documentation of the methodology and tools used to monitor configuration changes

4. Documentation of Minimum Security Configurations. The Minimum Security Configuration is the implementation of the Minimum Security Controls identified in

DOE CIO TMR-1, *Management, Technical, and Operational Controls*, and DOE M 205.1-4, *National Security System Manual*, and documented in the SSP.

a. Identify the Minimum Security Configurations.

(1) Organizations using Microsoft Windows XP™ and plan to upgrade to Vista™ must utilize the minimum common Federal security configurations available from NIST[1] or Defense Information Systems Agency (DISA) [2].

(2) All other Minimum Security Configurations must be selected from recognized sources of checklist-producing organizations, including NIST[3], the National Security Agency (NSA)[4], the DISA Security Technical Implementation Guides (STIGs), and the Center for Internet Security (CIS) benchmarks[5].

(3) The process for modifying the selected Minimum Security Configurations must be fully documented in the PCSP.

b. Specify Minimum Security Configurations in all information technology procurements.

TMR-8-2, Operating Unit Configuration Management Program

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

[1] The Microsoft Windows XP security configuration is available at http://csrc.nist.gov.itsec/download_WinXP.html, and the configuration for Microsoft Vista is available from http://csrc.nist.gov/itsec/guidance_vista.html.

[2] DISA's STIGs are available at http://iase.disa.mil/stigs/index.html.

[3] The NIST checklist repository is located at http://checklists.nist.gov/ .

[4] The NSA's checklists are available at http://www.nsa.gov/ia/.

[5] CIS's site is http://www.cisecurity.org/.