Cyber Security Technical and Management Requirements

Vulnerability Management (TMR-4)
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.

Vulnerability management is a measurable, proactive process implemented to secure information assets and improve regulatory compliance posture. This TMR establishes a risk-based vulnerability management 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) 800-40, *Creating a Patch and Vulnerability Management Program*, NIST SP 800-42, *Guideline on Network Security Testing*, NIST SP 800-51, *Use of Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, and NIST SP 800-55, *Security Metrics Guide for Information Technology 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-4, *Vulnerability Management Guidance*, dated July 28, 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-4-1, Senior DOE Management Vulnerability Management Program

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing vulnerability management for all operating units, programs, and systems.

The Senior DOE Management vulnerability management program is to include requirements for:

1. An inventory of information technology resources, including hardware, operating systems, and software applications used in the organization

2. Identification and dissemination of vulnerability information

3. Integration with Configuration Management (see DOE CIO TMR-8, *Configuration Management*), Incident Management (see DOE CIO TMR-9, *Incident Management*), and Risk Management (see DOE CIO TMR-3, *Risk Management*).

4. Remediation strategies and processes

5. Prioritization of vulnerability remediation

6. Vulnerability scanning

7. A standardized vulnerability naming scheme

8. The documentation of vulnerabilities, including Corrective Action Plans and POA&M documentation (see DOE CIO TMR-6, *Plans of Action and Milestones*).

9. Metrics for testing the effectiveness of the patch and vulnerability management processes

10. Communication and coordination procedures, including internal and external reporting of vulnerabilities and remediation

11. A process for identifying, documenting, and communicating lessons-learned concerning vulnerability scanning and remediation

TMR-4-2, Patch Management and Flaw Remediation

Senior DOE Management is responsible for defining, documenting in the PCSP, and implementing patch management and flaw remediation policies and procedures for all operating units, programs, and systems. The policies, processes, and procedures for the development, documentation, implementation, and management of patch management and flaw remediation processes must include at least the following:

1. Roles and responsibilities of all key personnel responsible for decisions and activities regarding patch and flaw remediation management

2. Patch prioritization and testing

3. Automated/ manual patch and flaw remediation deployment

4. Identification of those resources that cannot be patched from a central network location

5. Prioritization, coordination, and implementation of vulnerability remediation and/or mitigations

6. Testing and review of cyber security patches, updates, and corrective actions under Configuration Management procedures for security significant change impacts and risk mitigation.

   a. Maximum time(s) for security patch testing and installation.

   b. All patches and updates must be reviewed for operating unit applicability, system risk mitigation, and tested to ensure that system stability is maintained and existing applications and services are not negatively impacted.

   c. The Designated Approving Authority (DAA) must approve decisions not to apply security patches, as in the case where stability of the system may be sacrificed (and thus availability).

   d. Patches may be obtained from a number of sources, including CIAC (http://www.ciac.org/ciac/index.html), the US-CERT Web site (http://www.us-cert.gov), and trusted vendors.

7. Patch installation and flaw remediation verification processes and methods

8. Risk assessment and acceptance, approval, and communication

TMR-4-3 Vulnerability Scanning

Senior DOE Management is responsible for defining, documenting in the PCSP, and implementing vulnerability management policies and procedures for all operating units, programs, and systems. At a minimum, the policies, processes, and procedures for the development, documentation, implementation, and management of vulnerability scanning processes must include at least the following:

1. Risk-based standards establishing scan frequency, techniques, and technology(ies) for all National Security Systems (refer to DOE M 205.1-4, *National Security Systems Manual*). For scanning requirements for unclassified systems refer to DOE CIO TMR-1, *Management, Operational, and Technical Controls*.

2. Identification of the operating unit element(s) responsible for vulnerability scanning

3. The identification and prioritization of scanning targets

4. Identification of resources that cannot be scanned from a central network location

5. Alternate examination methodologies for resources for which operations/production cannot be interrupted (e.g., SCADA systems)

TMR-4-4 Operating Unit Vulnerability Management Policies and Procedures

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement vulnerability 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.