Cyber Security Technical and Management Requirements

External Information Systems (TMR-14)
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.

External Information Systems (EIS) are information technology resources and devices that are personally owned, corporately owned, or external to the system's accreditation boundary. This TMR establishes a risk-based approach that is to be covered in each PCSP for the secure use of External Information Systems for accessing, collecting, creating, processing, transmitting, disseminating, or storing DOE/Government information within and outside DOE security areas. 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-15, *Personally Owned Devices Guidance,* dated January 2007.

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-14-1, Senior DOE Management Requirements for External Information Systems

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing policies, processes, and procedures for the use of External Information Systems with unclassified Federal information systems for all operating units and programs. At a minimum, the Senior DOE Management PCSP is to address the following.

1. Identify, document, and assess business needs and circumstances under which use of External Information Systems can be authorized for collecting, creating, disseminating, accessing, processing, storing, and transmitting DOE/Government information.

2. Identify specific operational environments within which the use of External Information Systems will be permitted and the process to determine the network boundaries of these systems.

3. Identify conditions and define policies for allowing External Information Systems into areas where DOE unclassified information is being processed. These processes/procedures are to:

    a. Identify the controls used to reduce/eliminate the DOE TEMPEST/Technical Surveillance Countermeasures (TSCM) concerns (e.g., wireless, audio, video, infrared, etc.) when allowing the operation of these devices in security areas and

    b. Ensure that visitors to any area where Sensitive Unclassified Information (SUI) is being processed on cyber systems are advised of the requirements for the secure use of External Information Systems.

4. Identify the conditions and define the controls used to ensure that connection of External Information Systems is made only to an information system that is specifically accredited for External Information System connectivity (e.g., a firewall, VPN server, etc.).

5. Identify conditions and define policies for the use of External Information Systems to transmit, receive, process or store SUI to include the use of encryption capabilities conforming to DOE CIO TMR-22, *Protection of Sensitive Unclassified Information, including Personally Identifiable Information*.

6. Administrative procedures for enforcing the policy(ies) for the use of External Information Systems, including actions to be taken when such devices are used in a manner inconsistent with the PCSP.

7. Identify specific training or support requirements for External Information Systems, including training on protection of Government information, secure operation, individual rules of behavior, and consequences for rule violation.

TMR-14-2, Senior DOE Management Requirements for National Security Systems

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing any additional minimum security controls for National Security Systems for all operating units, programs, and systems. At a minimum, the Senior DOE Management PCSP is to define requirements for National Security Systems to:

1. Govern the use of External Information Systems in areas where classified data are discussed or processed.

2. Govern the disposition of External Information Systems that have been or are being used to access, collect, create, process, transmit, disseminate, or store classified information.

TMR-14-3, Operating Unit External Information Systems Policies and Procedures

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