Cyber Security Technical and Management Requirements

Peer-to-Peer (P2P) Networking (TMR-18)
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.

Peer-to-peer (P2P) technology, services, and applications are useful but introduce significant security risks that must be mitigated to maintain the security of DOE systems and networks. This TMR provides specific direction applicable to a risk-based approach for the secure use of (P2P) technology, services, and applications in the DOE environment. It also provides for the Departmental implementation of Office of Management and Budget Memorandum 04-26, *Personal Use Policies and "File Sharing" Technology*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information 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-23, *Peer-to-Peer (P2P) Networking Guidance*, dated December 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-18-1, Senior DOE Management Requirements for Peer-to-Peer Networking

Senior DOE Management is responsible for defining, documenting in the PCSP, and implementing policies and procedures for the use and management of Peer-to-peer (P2P) networking for all operating units, programs, and systems. At a minimum, the Senior DOE Management PCSP is to include the following.

1. The default condition is that P2P applications, technology, or services are not to be used on DOE systems that contain or process Sensitive Unclassified Information (SUI).

2. P2P applications present an unacceptable level of risk to any system or network that contains or processes classified information. Therefore, P2P applications are prohibited from being employed in any National Security System.

3. If the application of P2P technology or service is required, each application of the technology must be justified and approved by the Designated Approving Authority (DAA) during the Initiation Phase of Certification and Accreditation (C&A). The justification must, as a minimum, include the following:

    a. Description of the P2P protocol(s) and application(s).

    b. Risk assessments for systems where P2P technology or services are to be used.

    c. Identification of controls at the system and network levels to detect improper use and attempted evasion of security controls.

4. The following security controls are to be implemented on applications, system components, and networks that are part of, or may come into contact with, P2P applications, technology, or services. Implemented controls are to be documented and tested in all associated System Security Plans (SSPs) during the C&A process.

    a. Technical controls that do not allow the P2P server-client applications to automatically reply (e.g., Pong) to broadcasts for locating another server-client (e.g., Pings).

    b. Operational controls detailing procedures for handling and distributing information.

    c. Management controls describing the rules of behavior for the user.

    d. Protocols specific to P2P server-client applications are not passed between systems or on the network unless specifically authorized in the Interconnection Security Agreement for each system hosting a P2P server-client application.

    e. Technical controls that provide the capability for boundary protection services to detect and block unauthorized P2P applications, services, and software ports.

    f. P2P access controls that reflect the Information Types and Security Category of the system.

g. Technical controls that limit operation of a server-client application to downloading (pull) and does not accept remote writing to the disks on the system hosting the P2P application from another system or system component (push).

h. Technical controls that limit the ports authorized for use by P2P applications.

TMR-18-2, Operating Unit P2P Networking Policies and Procedures

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement policies and procedures related to P2P networking compliant with the requirements defined in the PCSP and commensurate with the level of security required for the organization’s environment and specific needs.