Cyber Security Technical and Management Requirements

Portable and Mobile Devices (TMR-13)
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.

This TMR provides specific direction applicable to a risk-based approach for the secure use of portable and/or mobile devices in the DOE environment and OMB and NIST guidance that is to be covered in each PCSP. In addition, this TMR establishes processes for the use of portable/mobile devices (e.g., notebook computers, personal digital assistants, etc.) 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-14, *Portable/Mobile 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-13-1, Senior DOE Management Portable/Mobile Requirements

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing policies, processes, and procedures for the use of portable/mobile devices for all operating units, programs, and systems, to include at least the following

1. Policies and processes governing the protection and use of portable/mobile devices that process, store, transmit, or disseminate DOE/Government Information.

2. Requirements for the protection and transportation of portable/mobile devices, components of portable computing devices (e.g., removable disk or disk drives, etc.), containing Sensitive Unclassified Information (SUI) or classified information.

3. Requirements ensuring that portable and/or mobile devices processing DOE/Government information are included in a System Security Plan (SSP) and subjected to the Certification and Accreditation (C&A process).

4. Specific training and support requirements for portable/mobile devices, including training on secure operation, rules of behavior, and consequences for rule violation.

5. Policies and processes governing the use of portable/mobile devices in close proximity to (e.g., in the same room as) information systems processing Government information (e.g. unclassified information, Sensitive Unclassified Information, or classified information) including the following:

   a. Portable/mobile devices used to process SUI or in any area where SUI is processed and taken outside the United States, other than the assigned user's primary work location, are sealed with Senior DOE Management-approved tamper-indicating devices prior to removal of the computing device from the user's primary location. The tamper-indicating devices must be placed to allow normal use (i.e., removal and insertion of components such as removable hard drives and batteries). The cognizant Designated Approving Authority (DAA) may approve alternative protection measures for operational requirements or when the use of tamper-indicating devices is ineffective.

   b. Portable/mobile devices used to process SUI or in any area where SUI is processed and taken outside the United States, other than the assigned user's primary work location, when tampering is indicated or tamper indicators could not be placed without interfering with normal use must be subjected to a hardware and/or software technical review process upon return to detect unauthorized software, firmware, or hardware changes.

   c. The operational environment and protections for each portable/mobile device is described in a SSP. The SSP must identify any restrictions and special security considerations for use in different security areas including at home or off-site:

      (1) May be used in or brought into an area where SUI is being processed in accordance with the policies and procedures defined in the PCSP and documented in the device's associated SSP only.

      (2) May connect to DOE or DOE contractor information systems processing DOE information only if allowed by the PCSP and the information system's SSP.

   d. Administrative and physical controls to reduce/ eliminate the DOE TEMPEST/ Technical Surveillance Countermeasure (TSCM) concerns when allowing the

operation of portable/ mobile devices with a wireless, audio, or video recording capability in security areas must be documented in the SSP.

e. A process to ensure that visitors to any area where DOE SUI or classified information is being processed on cyber systems are advised of the requirements for the secure use of portable/ mobile devices.

TMR-13-2, Senior DOE Management Requirements for National Security Systems

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing minimum security controls in addition to DOE M 205.1-4 for portable/mobile devices that host classified information or are used in an area where classified information is processed. At a minimum, the Senior DOE Management PCSP is to define additional requirements for National Security Systems to ensure that:

1. All portable/ mobile devices that process, display, store, or transmit classified information are to comply with TEMPEST (Study of Compromising Emanations), Protected Transmission System, and TSCM policies.

2. Portable/ mobile devices accredited for classified processing are prohibited from:
   a. Downloading or loading any shareware, extraneous software, or unauthorized freeware.

   b. Synchronizing with any unclassified system.

3. Policies and processes for approving where portable/mobile devices will be permitted including the following:
   a. Portable/mobile devices used to process classified information or in any area where classified information is processed and taken outside the United States, other than the assigned user's primary work location, are sealed with Senior DOE Management-approved tamper-indicating devices prior to removal of the computing device from the user's primary location. The tamper-indicating devices must be placed to allow normal use (i.e., removal and insertion of components such as removable hard drives and batteries). The cognizant Designated Approving Authority (DAA) may approve alternative protection measures for operational requirements or when the use of tamper-indicating devices is ineffective.

   b. Portable/mobile devices used to process classified information or in any area where classified information is being processed and have been taken outside the United States, other than the assigned user's primary work location, are subjected to a hardware and software technical review process upon return to detect unauthorized software, firmware, or hardware changes.

TMR-13-3, Operating Unit Portable & Mobile Device Policies and Procedures

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