Cyber Security Technical and Management Requirements

Wireless Devices and Information Systems (TMR-12)
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.

This TMR establishes a risk-based approach that is to be covered in each PCSP for the secure use of unclassified and National Security wireless devices and information systems within the DOE. It also provides for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices,* and NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.* Senior DOE Management may specify and implement additional requirements in each PCSP to address specific risks, vulnerabilities, or threats within its operating units.

For the purposes of this TMR, Wireless Information Systems (WIS) include wireless telecommunication or computer-related equipment, or interconnected systems or subsystems of equipment (including software, firmware, and hardware) used to support DOE business, operations, and missions in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data. The WIS technology excludes tactical radios; mobile satellite systems; and land mobile, emergency, and one-way receive-only devices.

Cancellations

This TMR replaces DOE CIO Guidance CS-13, *Wireless Devices and Information Systems Guidance,* dated June 30, 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-12-1, Senior DOE Management Wireless Requirements

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing requirements for the use and management of wireless information systems for all operating units, programs, and systems. The Senior DOE Management PCSP must include the following requirements.

1. Roles and responsibilities of all key personnel responsible for approval, implementation, and oversight of wireless networks or devices.

2. Requirements for evaluating and justifying the business needs for deploying wireless information systems (e.g., cost/benefit analysis, availability and feasibility of more secure technologies) and approving if and where wireless access, applications, and systems will be permitted.

3. Requirements for assessment of the risks to the confidentiality, integrity, and availability of operating unit information resources in the context of wireless networking devices to include the entire spatial volume of transmitted/received signal capability.

4. Minimum security controls for wireless devices and networks of information systems.

5. Minimum security controls to manage risks associated with portable computers with wireless networking capabilities.

6. Minimum security controls[1] for wireless systems located in the proximity of sensitive unclassified or classified information processing areas, including those using FIPS 140-1 and 140-2 encryption products.

7. Minimum security controls for interconnection of wireless networks to DOE Local Area Network (LAN) or Wide Area Network (WAN) Services and information systems.

8. Identification of conditions and definition of policies for introducing wireless portable/mobile systems into areas where unclassified and classified information is being processed. These processes/procedures are to address:

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

[1] In areas subject to recurring Technical Surveillance Countermeasure (TSCM) services, the introduction of wireless devices requires approval based on the requirements of the DOE TSCM manual and DOE M 470.4-4, *Information Security*.

b. The controls used to ensure that interconnection of wireless portable/ mobile systems is made only to an information system that is accredited for the interconnection; and

c. Personnel training on the policies, processes, and procedures for the use of wireless portable/ mobile systems and protection of Government information.

TMR-12-2, Senior DOE Management Requirements for National Security Systems

Senior DOE Management must develop, document in the PCSP, and implement requirements for the use and management of wireless devices and information systems for all operating units, programs, and systems. The Senior DOE Management PCSP must include the following requirements:

1. Wireless devices accredited for use in National Security Systems are not used:
   a. To download or load any shareware, extraneous software, or unauthorized freeware and

   b. To synchronize with any unclassified system.

2. Wireless networks used to transmit national security information must:
   a. Support security for voice, data, and control channel information only via approved Type 1 encryption for all modes of operation;

   b. Be monitored to detect unencrypted signals transmitted from areas where classified information is being electronically stored, processed, or transmitted to ensure unauthorized signals are not transmitted beyond approved boundaries;

   c. Use security mechanisms that are compatible and interoperable with those mechanisms used on wired voice and data telecommunications networks and computing devices; and

   d. Implement identification and authentication measures at both the device and network level.

TMR-12-3, Operating Unit Wireless Policies and Procedures

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