

**U.S. Department of Energy
Cyber Security Program**

**WIRELESS DEVICES AND
INFORMATION SYSTEMS
GUIDANCE**



June 30, 2006

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides direction for the use of unclassified and National Security wireless devices and information systems within the DOE, including the National Nuclear Security Administration (NNSA), and the implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*.

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.

This Guidance provides additional information to Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance* and DOE CIO Guidance CS-22, *National Security Systems Controls Guidance*, in their Program Cyber Security Plans (PCSPs). Specifically, this Guidance applies to Access Control (AC)-18 in CS-1 and System Assurance controls in CS-22.

The DOE CIO will review this Guidance annually and update it as necessary. The Senior DOE Management, and their operating units may provide feedback at any time for incorporation into the next scheduled update.

2. CANCELLATIONS.

None.

3. APPLICABILITY.

- a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to which DOE CIO Guidance CS-13 is Applicable*.

Further, the DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE CIO (hereinafter referred to as Senior DOE Management) may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their subordinate organizations and contractors (hereinafter called operating units), and for ensuring that those requirements are incorporated into contracts.

- b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency

through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.

- c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.
- d. National Security Systems. Senior DOE Management Program Cyber Security Plans (PCSPs) are to address this Guidance, Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program, the requirements of the National Industrial Security Program Operating Manual (NISPOM), and DOE M 471.2-2, *Classified Information Systems Security Manual*, for all DOE National Security information systems. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

4. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its effective date. If Senior DOE Management cannot address all of the criteria by the scheduled milestone, DOE expects Senior DOE Management to establish a Plan of Actions and Milestones (POA&Ms) for implementation of this Guidance into their PCSP.

5. CRITERIA.

- a. Program Cyber Security Plans. Senior DOE Management PCSPs are to be consistent with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement wireless devices and information system policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs
 - (1) Define roles and responsibilities of all key personnel responsible for approval, implementation, and oversight of wireless networks or devices into the environment.
 - (2) Define processes for evaluating the business needs for deploying wireless information systems, to include cost/benefit analysis and whether more secure technologies (e.g., expansion of wired network) are feasible.

- (3) Define process 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) Identify specific environments within which wireless access will be permitted, and the process to determine the network boundaries of the systems that will permit wireless access.
 - (5) Establish minimum security controls¹ for wireless systems located in the proximity of sensitive unclassified or classified information processing areas, including the use of FIPS 140-1 and 140-2 encryption products.
 - (6) Define processes for approving where wireless access, applications, and systems will be permitted.
 - (7) Establish minimum security controls, and testing requirements for the controls, to be enforced for wireless devices and networks of information systems, including controls to manage risks associated with portable computers with wireless networking capabilities.
 - (8) Establish minimum security controls for interconnection of wireless networks to DOE Local Area Network (LAN) or Wide Area Network (WAN) Services and information systems.
 - (9) Define methods to detect intrusion into wireless networks and rogue wireless devices.
 - (10) Identify specific training or support requirements for wireless devices and networks, including training on secure operation, individual rules of behavior, and consequences for rule violation.
 - (11) Establish a Certification and Accreditation process for wireless systems and devices.
 - (12) Define incident detection and handling processes when wireless technology may be involved.
- b. Additional Criteria for National Security Systems. Wireless-enabled information technology must protect the National Security information it processes, stores, displays, or transmits and that of any conventional wire-based infrastructure to which it interconnects as classified under (i) the Atomic Energy Act of 1954, as amended; (ii) E.O. 12958, Classified National Security Information, dated April 17, 1995, and amended March 25, 2003; and (iii) applicable Director of Central Intelligence Directives.

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*.

- (1) Ensure that data streams transmitted over wireless devices use National Security Agency (NSA) Type 1 end-to-end encryption for secure transmission of classified information when—
 - (a) Connected to National Security networks or computers;² or
 - (b) Used by Senior DOE Management and operating unit personnel or Senior DOE Management- or operating unit-authorized contractors for supporting classified DOE business.
- (2) Ensure that wireless devices accredited for use in National Security information systems are not used—
 - (a) To download or load any freeware, shareware, or any extraneous software;
 - (b) To synchronize with any unclassified system; or
 - (c) Without NSA-approved cryptography.
- (3) Ensure wireless networks—
 - (a) Support security for voice, data, and control channel information only via approved Type 1 encryption for all modes of operation;
 - (b) Are 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;
 - (d) Are configured to protect against unauthorized access through the use of strong identification, authentication, and auditing; and
 - (e) Implement identification and authentication measures at both the device and network level.

6. REFERENCES.

References are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

² Devices that have wireless ports that do not support Type 1 end-to-end encryption but use the wire-line port are permitted only if the wireless port is disabled (for example, printers that have wireless ports).

7. DEFINITIONS.

Terms specific to this Guidance are defined in Attachment 2. Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

8. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO
GUIDANCE CS-13 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2GLOSSARY

End-to-End Encryption. Encryption of information at its origin and decryption at its intended destination without intermediate decryption.

Land Mobile Radio. Conventional portable systems that dedicate a single radio channel to a specific group of users who share it. These portable communication devices typically operate at the following frequency bands: very high frequency (VHF) low band, VHF high band, and ultrahigh frequency (UHF). Adjacent channel spacing is typically 20 kilohertz (kHz) for low band; 12.5, 25, or 30 kHz for high band; and 12.5 or 25 kHz for UHF. **Local Area Network (LAN) Services.** Services provided by connecting to servers within a confined geographic area.

Mobile Satellite Systems (MSS). Networks of communications satellites intended for use with mobile and portable wireless telephones or computing devices. There are three major types: AMSS (aeronautical MSS), LMSS (land MSS), and MMSS (maritime MSS). A connection using MSS is similar to a cellular link, except the repeaters are in orbit around the earth rather than on the surface. MSS repeaters can be placed on geostationary, medium earth orbit, or low earth orbit satellites. Provided there are enough satellites in the system, and provided they are properly spaced around the globe, an MSS can link any two wireless devices at any time, no matter where in the world they are located. MSS systems are interconnected with land-based cellular networks.

Portable Computing Device. Device that provides capability to collect, create, process, transmit, store, and disseminate information. These devices include (but are not limited to) personal digital assistants, palmtops, handheld or portable computers and workstations, non-Web-enabled cell phones, Web-based enhanced cell phones, two-way pagers, and wireless e-mail devices.

Type 1 Encryption Product. Classified or controlled cryptographic item endorsed by the National Security Agency (NSA) for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products and not to information, key, services, or controls. Type 1 products contain approved NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulations.

Wide Area Network (WAN) Services. Services provided by connecting to servers within a large geographic area (state or country) often connecting multiple LANs.