U.S. Department of Energy
Washington, D.C.

NOTICE

DOE N 205.8

Approved: 2-11-04
Expires: 2-11-05

SUBJECT: CYBER SECURITY REQUIREMENTS FOR WIRELESS DEVICES AND INFORMATION SYSTEMS

1. OBJECTIVES.

   a. To establish Department of Energy (DOE) policy requirements and responsibilities for using wireless devices and information systems within DOE.

   b. To implement the applicable requirements of section 4 of DOE O 205.1, *Department of Energy Cyber Security Management Program*, dated 3-21-03, including requirements for cyber resource protection, risk management, program evaluation, and cyber security plan development and maintenance.

   c. To fulfill the commitment to performance-based management of DOE contracts as outlined in Secretary Abraham's May 12, 2003, memorandum, *Clarification of Roles and Responsibilities,* by supporting to the "maximum extent practicable, the principle to apply performance-based contracting techniques under which the contract will define what is to be done, and not how it will be done."

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. DOE Organizations. Except for the exclusions in paragraph 3d, this Notice applies to Primary DOE, including National Nuclear Security Administration (NNSA), Organizations that own or operate DOE information systems or national security systems [1] (see Attachment 1 for a complete list of Primary DOE Organizations). The attached list automatically includes any Primary DOE Organizations created after this Notice is issued.

   b. Site/Facility Management Contractors. Except for the exclusions noted in paragraph 3d, the Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Notice that will apply to site/facility management contractors whose contracts include the CRD.

      (1) This CRD must be included in site/facility management contracts that provide automated access to DOE information systems (see Attachment 3).

      (2) This Notice does not automatically apply to other than site/facility management contractors. Any application of requirements of this Notice

[1] As defined in National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System,* dated August 2003.

to other than site/facility management contractors will be communicated separately from this Notice.

(3) Heads of Primary DOE Organizations are responsible for informing their appropriate contracting officers which site/facility management contractors are affected by this Notice. Once notified, contracting officers are responsible for incorporating the CRD into the contracts of affected site/facility management contractors via the laws, regulations, and DOE directives clauses of the contracts.

(4) As the laws, regulations, and DOE directives clause of site/facility management contracts states, regardless of the performer of the work, site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD.

(a) Affected site/facility management contractors are responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

(b) Contractors must not unnecessarily or imprudently flow down requirements to subcontractors. That is, contractors will—

1 ensure that they and their subcontractors comply with the requirements of this CRD and

2 incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

c. DOE O 205.1 establishes the Office of the Chief Information Officer as having responsibility for all cyber security policies and guidelines, including wireless devices and information systems documented in existing DOE policies.

d. Exclusions.

(1) Consistent with the responsibilities identified in Executive Order (E.O.) 12344, Naval Nuclear Propulsion Program, dated February 1, 1982, 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 Notice for activities under the Deputy Administrator's cognizance.

(2) Land mobile radios or mobile satellite services are excluded from this Notice.

4. REQUIREMENTS.

a. Background. The National Institute of Standards and Technology has described the use of wireless communications and technologies as follows.

"Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (LAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Wireless micro-LAN functionality also eliminates cables for printers and other peripheral device connections. Handheld devices such as personal digital assistants and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the equivalent of an Ethernet port in a parking lot."[2]

Additionally, devices that enable portable computing are in many instances replacing many traditional computer functions. These devices are very small, easily transportable, and designed to store significant amounts of information, making them popular for all levels within the organization. However, these devices currently have few built-in security features. Those that contain password protection allow the user to bypass that feature. The storage capability of these devices has increased markedly, and many devices now support removable media cards and memory sticks. As portable computing devices become more prominent, the risk to the workplace environment increases. Virus writers and other hackers have begun to target nonsecure wireless devices that exchange information directly with workstations. When a user synchronizes a device to a desktop computer, a virus can be unwittingly transferred even when the device itself is unaffected.

Currently, most commonly sold portable computing devices have radio frequency (RF) transmission capabilities, and almost all devices are equipped with infrared ports that can be used for high-speed information exchange. RF capability is

[2] Excerpted from National Institute of Standards and Technology Special Publication 800-48 *Wireless Network Security 802.11, Bluetooth and Handheld Devices,* dated November 2002.

becoming more prominent. The compact nature of these devices makes them of particular concern for unauthorized use.

b. Implementation. DOE organizations must implement the requirements and meet the responsibilities contained in this Notice within 90 days of its issuance. This Notice must be implemented at all organizational levels. Requirements and responsibilities will flow down, as appropriate, from the heads of Primary DOE Organizations to all subordinate organizational levels.

c. Risk Management. In implementing this Notice, DOE Organizations must use a documented, risk-based approach consistent with the principles and guidelines of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, dated November 2002, to make informed decisions for using wireless devices and information systems, including documenting decisions on the adequacy and maintenance of security controls, cost implications of enhanced protection, and acceptance of residual risk by heads of Primary DOE organizations.

d. Program Cyber Security Plan (PCSP) Requirements. DOE Organization PCSPs will document the following.

(1) Roles and responsibilities of all key personnel responsible for the decision to incorporate wireless networks or devices into the environment.

(2) The process to determine the network boundaries of the systems that will have wireless access.

(3) Capital planning issues related to whether to incorporate wireless technologies into the environment, including incorporating and funding security over the life cycle of individual systems as required by the Federal Information Security Management Act of 2002.

(4) Identification of the minimum security controls that are to be enforced for wireless devices and networks of information systems.

(5) Identification of the minimum security controls for interconnection of wireless networks to DOE LANs, wide area networks, and services to information systems.

e. Cyber Security Program Plan (CSPP) Requirements. DOE Organization CSPPs will document the following.

(1) Roles and responsibilities of all key personnel responsible for the decision to incorporate wireless networks or devices into the environment.

(2) Specific environments within which wireless access will be permitted.

(3) Ensured compliance with TEMPEST (Study of Compromising Emanations), protected transmission system, and technical surveillance countermeasures for all wireless systems processing national security information.

(4) Applications and systems within which wireless access will be permitted.

(5) Specific technical, operational, and management controls necessary to maintain risk at an acceptable level and the schedule for testing such controls to ensure they continue to operate as intended, with specific reference to setup and configuration standards for security, addressing, and access options for each allowed device type.

(6) Specific training or support requirements for the wireless devices and networks, including training on individual rules of behavior and consequences for rule violation.

f. Significant Changes. As described in DOE O 205.1 and Office of Management and Budget (OMB) Circular A-130, Appendix III, significant changes in the level of risk may result when new technologies or operational procedures are introduced into information systems; for example, when wireless devices or networks are incorporated into a wired legacy information system.

(1) Consistent with procedures set forth in applicable PCSPs and CSPPs, when the introduction of new technologies or procedures causes a significant increase in the level of risk, system-level security plans and authorization to process (i.e., certification and accreditation) must be updated to reflect the increased risk and include revised risk mitigation methods.

(2) OMB Circular A-130, Appendix III, requires that a management official authorize in writing the use of a system based on implementation of its security plan before beginning or significantly changing system operations.

(3) Consistent with the roles and responsibilities set forth in applicable PCSPs and CSPPs, owners and operators of interconnected applications and systems must be notified of significant changes that can impact their interconnection agreements.

For example, when operational DOE or contractor applications or systems that use wireless technologies do not meet the above requirements, the weaknesses must be documented and addressed in applicable corrective

action plans and milestones. Threat statements, system risk assessments, and mitigation plans must be updated before incorporating wireless technology into an approved system boundary.

5. ADDITIONAL REQUIREMENTS FOR NATIONAL SECURITY SYSTEMS.

a. 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 (1) the Atomic Energy Act of 1954, as amended; (2) E.O. 12958, Classified National Security Information, dated April 17, 1995, and amended March 25, 2003; and (3) applicable Director of Central Intelligence directives, as reflected in applicable PCSPs. In addition, only wireless devices that meet National Security Agency (NSA) requirements for Type 1 end-to-end encryption for the secure transmission of classified information will be—

(1) connected to classified networks or computers;[3]

(2) used as mission critical systems;

(3) used as primary means of communications for mission operations; or

(4) used by DOE personnel or DOE-authorized contractors for supporting classified DOE business.

b. Wireless devices that are accredited for classified processing must not be—

(1) used to download or load any freeware or shareware enhancements or any extraneous software;

(2) used to synchronize any unclassified system;

(3) used in areas where classified data are discussed or processed without approval of the designated approving authority;[4] or

(4) used without NSA-approved cryptography for file encryption, if the wireless device has file encryption capabilities.

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

[4]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 473.1-1, *Physical Protection Program Manual,* dated 12-23-02.

c. Wireless networks will—

(1) support security for voice, data, and control channel information via approved Type 1 end-to-end encryption for all modes of operation;

(2) be monitored to detect the signals transmitted from areas where classified information is being electronically stored, processed, or transmitted unencrypted to ensure unauthorized signals are not being transmitted beyond approved boundaries;

(3) use security mechanisms that are compatible and interoperable with those mechanisms used on wired voice and data telecommunications networks and computing devices; and

(4) be configured to protect against unauthorized access through the use of strong identification, authentication, and auditing.

(a) Personal identification and strong authentication mechanisms are required for access to DOE information systems in accordance with DOE policy.

(b) Identification and authentication measures will be implemented at both the device and network level.

6. DEFINITIONS. See Attachment 4 for definitions relevant to this Notice.

7. REFERENCES.

a. The following public laws and policies contain cyber security program requirements and guidance that may be helpful in implementing this Notice.

(1) Atomic Energy Act of 1954, as amended.

(2) E.O. 12958, Classified National Security Information, dated April 17, 1995, and amended March 25, 2003.

(3) E.O. 12344, Naval Nuclear Propulsion Program, dated February 1, 1982.

(4) OMB Circular A-130, *Management of Federal Information Resources*, dated November 2000.

(5) The Paperwork Reduction Act of 1995, as amended.

(6) Public Law 107-347, E-Government Act of 2002; Title III—Information Security (also known as the Federal Information Security Management Act of 2002), dated December 17, 2002.

b. The following national standards and guidelines provide relevant processes and procedures for implementing this Notice.

(1) NIST Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules,* amended December 3, 2002.

(2) NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System,* dated August 2003.

(3) NIST SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices,* dated November 2002.

c. The following DOE directives provide relevant requirements and procedures for implementing this Notice.

(1) DOE G 205.3-1, *Password Guide,* dated 11-23-99.

(2) DOE M 473.1-1, *Physical Protection Program Manual,* dated 12-23-02.

(3) DOE M 471.2-2, *Classified Information Systems Security Manual*, dated 8-03-99.

(4) DOE M 471.2-1C, *Classified Matter Protection and Control Manual*, dated 4-17-01.

(5) DOE N 205.3, *Password Generation, Protection, and Use,* dated 11-23-99.

(6) DOE O 471.2A, *Information Security Program,* dated 3-27-97.

(7) DOE O 205.1, *Department of Energy Cyber Security Management Program*, dated 3-21-03.

8. CONTACT. Questions concerning this Notice should be directed to the Office of the Chief Information Officer, Office of Cyber Security, at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

PRIMARY DOE ORGANIZATIONS TO WHICH DOE N 205.8 IS APPLICABLE

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
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 Security
Office of Security and Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Secretary of Energy Advisory Board
Office of Independent Oversight and Performance Assurance
Office of Legacy Management
Office of Energy Assurance
Office of Electric Transmission and Distribution
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT
DOE N 205.8 *Cyber Security Requirements for Wireless Devices and Information Systems*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration contractors, with access to DOE information systems. Contractors must comply with the requirements listed in the CRD.

This CRD supplements requirements contained in the CRD for DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03, including requirements for cyber resource protection, risk management, program evaluation, and cyber security plan development and maintenance.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor must not unnecessarily or imprudently flow down requirements to subcontractors. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

The contractor must ensure that all wireless devices and information systems used by its employees or at facilities under its control satisfy or comply with the requirements listed below.

1. RISK MANAGEMENT. The contractor must use a risk-management approach in protecting information and information systems. A documented risk-management approach consistent with the principles and guidelines of National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices,* dated November 2002, must be used to support decisions to incorporate wireless technologies related to the adequacy of protection, cost implications of further enhanced protection, and the acceptance of residual risk. Security controls must be continuously monitored to ensure they continue to operate as intended.

2. NATIONAL SECURITY SYSTEMS.[1]

   a. 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—

      (1) the Atomic Energy Act of 1954, as amended;

[1]As defined in National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System,* dated August 2003.

(2) E.O. 12958, Classified National Security Information, dated April 17, 1995, and amended March 25, 2003, and

(3) applicable Director of Central Intelligence directives, as reflected in applicable Program Cyber Security Plans.

b. In addition, only wireless devices that meet National Security Agency (NSA) requirements for Type 1 end-to-end encryption for the secure transmission of classified information will be—

(1) connected to classified networks or computers,[2]

(2) used as mission critical systems,

(3) used as primary means of communications for mission operations, or

(4) used for supporting DOE classified business.

c. Wireless devices that are accredited for classified processing must not be—

(1) used to download or load any freeware or shareware enhancements or any extraneous software;

(2) used to synchronize with any unclassified system;

(3) used in areas where classified data are discussed or processed without approval of the designated approving authority;[3] or

(4) used without NSA-approved cryptography for file encryption, if the wireless device has file encryption capabilities.

d. Wireless networks will—

(1) support security for voice, data, and control channel information via approved Type 1 end-to-end encryption for all modes of operation;

(2) be monitored to detect the signals transmitted from areas where classified information is being electronically stored, processed, or transmitted unencrypted to ensure unauthorized signals are not being transmitted beyond approved boundaries;

---

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

[3]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 473.1-1, *Physical Protection Program Manual,* dated 12-23-02.

(3) use security mechanisms that are compatible and interoperable with those mechanisms used on wired voice and data telecommunications networks and computing devices; and

(4) be configured to protect against unauthorized access through the use of strong identification, authentication, and auditing.

(a) Personal identification and strong authentication mechanisms are required for access to DOE information systems in accordance with DOE policy.

(b) Identification and authentication measures will be implemented at both the device and network level.

CONTRACTOR REQUIREMENTS DOCUMENT (CRD) APPLICABILITY

The CRD for DOE N 205.8, *Cyber Security Requirements for Wireless Devices and Information Systems,* dated 2-11-04, is intended to apply to the site/facility management contracts applicable to the following sites/facilities.

Lawrence Berkeley National Laboratory

Pacific Northwest National Laboratory

Brookhaven National Laboratory

Sandia National Laboratories

National Renewable Energy Laboratory

Stanford Linear Accelerator Center

Bettis Atomic Power Laboratory

Argonne National Laboratory

Idaho National Engineering & Environmental Laboratory

Thomas Jefferson Nat'l Accelerator Facility

Ames National Laboratory

Oak Ridge National Laboratory

Knolls Atomic Power Laboratory

Lawrence Livermore National Laboratory

Los Alamos National Laboratory

Savannah River Site

Princeton Plasma Physics Laboratory

Fermi National Accelerator Center

West Valley Project

Strategic Petroleum Reserve

Oak Ridge Y-12 National Security Complex

Pantex Plant

Waste Isolation Pilot Plant

Nevada Test Site

Kansas City Plant

National Civilian Radioactive Waste Program (Yucca Mountain)

Hanford Environmental Restoration

Oak Ridge Environmental Management

Mound Environmental Management Project

Project Hanford

River Protection Project Tank Farm Management

Rocky Flats

Fernald Environmental Management Project

Grand Junction Technical & Remediation Services

Grand Junction Facilities & Operations Services

Oak Ridge Institute of Science & Education

Occupational Health Services at the Hanford Site

DEFINITIONS

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 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 local area networks.

Wireless Information Systems. Wireless telecommunication or computer-related equipment or interconnected systems or subsystems of equipment (includes software, firmware, and hardware). This equipment is 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. WIS excludes tactical radios and land mobile; emergency; and one-way, receive-only devices.