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

NOTICE

DOE N 205.11

Approved: 2-19-04
Expires: 2-19-05

SUBJECT: SECURITY REQUIREMENTS FOR REMOTE ACCESS TO DOE AND APPLICABLE CONTRACTOR INFORMATION TECHNOLOGY SYSTEMS

1. OBJECTIVES.

   a. To establish Department of Energy (DOE) policy requirements and responsibilities for remote connection to DOE and contractor information technology systems.

   b. To implement the requirements of DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03, to protect DOE information and information systems commensurate with the risk and magnitude of harm that could result from their unauthorized access, use, disclosure, modification or destruction.

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

   b. Site/Facility Management Contractors. Except for the exclusions in paragraph 3c, 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) The CRD must be included in site/facility management contracts that provide automated access to DOE information systems. (Site/facility Management contractors to which this CRD applies are listed in Attachment 3).

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

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

(3) Lead Program Secretarial Officers are responsible for telling 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 contracts of affected site/facility management contractors via the laws, regulations, and DOE directives clause of their 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 requirements of the CRD.

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

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

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

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

c. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, 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.

4. REQUIREMENTS.

Remote access to DOE and contractor information technology systems can promote cost-effective benefits to the DOE mission and workforce. At the same time, remote access can introduce significant risk to those systems.

Federal law and implementing policies require Agencies to develop, document, and implement programs to assess the risk and magnitude of harm that could result from

unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support Agency operations and assets.

Based upon a documented risk-based approach, an Agency must provide adequate security to maintain an acceptable level of risk to Agency operations and assets, including those provided or managed by another Agency, contractor, or other source.

Consistent with those requirements, this Notice sets forth minimum requirements for security of remote access to DOE and contractor information technology systems.

NOTE: This Notice does not address risks associated with or policy considerations specific to wireless networks and devices. Policies and procedures for these are addressed in DOE Notice 205.8, *Cyber Security Requirements for Wireless Devices and Information Systems*, dated 2-11-04.

a. Implementation. Primary DOE Organizations must implement the requirements of this Notice within 90 days of its issuance. These requirements must be implemented at all organizational levels as required by DOE O 205.1. Requirements and responsibilities will flow down from the heads of Primary DOE Organizations to all organizational levels.

b. Risk Management. Consistent with law and policy, Primary DOE Organizations must use a documented risk-based approach to make informed decisions regarding the use of remote access, implementing necessary security controls, and determining the acceptable level of residual risk. This risk-based approach must be consistent with the principles and guidelines of in National Institute of Standards and Technology Special Publication (NIST SP) 800-30, Risk Management Guide for Information Technology Systems, dated October 2001.

c. Remote Access Services. The following apply to Primary DOE Organizations' remote access services.

(1) A documented risk-based approach must be used for DOE or contractor information technology systems to determine the potential risk associated with system exposure to each user class identified in paragraph 4c(2)(b), below.

(2) Two principles apply.

(a) Remote access is granted based on valid business and user needs, including scientific and other collaborative activities.

(b) Least privilege is based on user classification (i.e., remote access must be limited to the minimum privileges required by an employee's user class).

1 General user—accesses only general services on the system for which remote access is authorized.

2 Privileged user—has access to high-level services (e.g., system administration, special read, write, delete, or configuration change privileges) on the system for which remote access is authorized.

3 Foreign national users—access is described in DOE N 205.2, *Foreign National Access to DOE Cyber Systems,* dated 11-01-99, or successor directives, and as detailed in the Primary DOE Organization's program cyber security plan (PCSP).

(3) User IDs and passwords must conform to DOE N 205.3, *Password Generation, Protection, and Use,* dated 11-23-99, or successor directives. DOE sites will not utilize clear-text, reusable passwords for remote access.

(4) Security-enabled transmission capabilities must be implemented to the maximum extent possible.

(5) Access will be granted only for authorized activities as identified within the Primary DOE Organization's PCSP.

(6) Officials responsible for remote access systems must provide continuous intrusion detection monitoring and must test the system at least annually to ensure continued adequate security regardless of the specific controls implemented.

d. Significant Changes. As described in DOE O 205.1 and OMB Circular A-130, Appendix III, significant change may result from the introduction of new technologies or operational procedures into information systems; for example, incorporating wireless devices or networks into a wired legacy information system.

(1) When introduction of new technology or procedures causes a significant change in the level of risk, system level security plans must be updated to reflect the increased risk, the risk mitigation techniques, and methods to be used. If introducing new technologies or processes increases level of risk, existing authorizations to process for that system or application (for example, certification and accreditation) are invalidated.

(2) According to OMB Circular A-130, Appendix III, a management official must authorize in writing the use of a system based on

implementation of its security plan before beginning operations or when a significant change occurs.

(3) Owners and operators of interconnected applications and systems must be notified of significant changes that can affect 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.[1]

Remote access to national security systems can be authorized when proper physical, personnel and cyber security controls are implemented at the host and remote sites in a manner prescribed by DOE and national security policies. In particular, all DOE Organizations must use certified, accredited systems which use National Security Agency Type 1 approved encryption or information assurance enabled products conforming to policies set forth in National Security Telecommunications and Information Systems Security Policy, (NSTISSP) 11, *National Information Assurance Acquisition Policy,* dated June 2003. The Designated Approving Authority (DAA) must issue an Interim Authority To Operation (IATO) or Authority To Operate (ATO) before systems can become operational.

6. MINIMUM SECURITY CONTROLS.

The following are minimum controls for management, technical, and operational controls. As required by law, OMB policy, and NIST standards, the following requirements apply to DOE information technology systems and contractor systems that store or process DOE information or support DOE operations and assets.

a. Management Controls.

(1) Document automated tools (e.g., firewalls, virtual private networks, encryption, intrusion detection, anti-virus software, and audit log analysis) provided to manage remote access services.

(2) Document procedures to report and respond to remote access security incidents.

(3) Document procedures to conduct random security evaluation of remote access controls.

---

[1]As defined in NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

(4) Describe rules of behavior and consequences for violations for all classes of users authorized for remote access.

(5) Address specific security and awareness training for those authorized to use remote access services.

b. Operational Controls.

(1) Provide individuals with the minimum requirements for operating system and application software for employees who use personal equipment to connect remotely to DOE networks.

(2) Individuals granted remote access privileges must commit to understanding and acknowledging minimum requirements and DOE remote access rules of behavior.

(3) Ensure that risks associated with the potential use of split-tunneling or other external services to conduct official DOE business are addressed and documented so that the appropriate controls are instituted and monitored for continued effectiveness.

c. Technical Controls.

(1) Document acceptable levels and types of authentication, and personal identification for remote access.

(2) Document procedures to ensure virus protection on remote equipment.

(3) Establish minimum requirements for the operating system and application software and for controlling and safeguarding Government-issued cryptographic keying material on all government and personal equipment used for remote access.

(4) Describe the process for organizations and users to obtain approval from system and data owners prior to implementing remote network access.

(5) Document procedures to ensure updates of security-related software patches and/or hardware updates on remote equipment.

7. RESPONSIBILITIES.

a. Office of the Chief Information Officer (OCIO).

(1) Develops and maintains Departmental cyber security Policies, Orders, Manuals, and guidelines for remote access services as required by DOE O 205.1.

(2) Provides strategic direction for managing remote access to information systems.

(3) Monitors the development of acquisition strategies and coordinates with Primary DOE Organizations to assess potential architectures that promote cost-effective acquisition, operation, and use of remote access equipment to permit efficiencies and interoperability.

(4) Provides oversight of remote access training by DOE Organizations.

b. Office of Security. Coordinates with the OCIO a consistent approach to protecting the DOE information assets and avoiding duplication of effort.

c. Heads of Primary DOE Organizations (see Attachment 1). Note that the authority for these actions may be reassigned.

(1) Ensure that remote access security requirements are addressed in the organization's PCSP and site-level cyber security program plans (CSPPs). (NOTE: Minimum requirements for security controls are described in paragraph 6. Specific rules of behavior for each class of user and consequences for violations of these rules must be documented. This information must be referenced or included in the PCSP and CSPP.)

(2) Ensure that remote access services are controlled and that user profiles are managed to reflect user class and job responsibilities.

(3) Ensure that a review of remote access security controls is documented and continuously monitored to ensure that they continue to operate as intended.

(4) Ensure that remote access issues, vulnerabilities, requirements, and technology changes are incorporated into training for all affected DOE and contractor personnel, including as appropriate the permitted extent of personal use.

(5) Ensure that guidance on remote access threats, vulnerabilities, and risks as defined in the Primary DOE Organization's PCSP is provided to designated approving authorities and is consistent with DOE policies and directives.

(6) Ensure that identified weaknesses in remote access controls, policies, and procedures are documented in the applicable security plan.

(7) Address conditions or limits on system interconnections and define service provision and restoration priorities including continuity of system operations.

8. REFERENCES.

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

(1) Public Law (P.L.) 107-347, E-Government Act of 2002, Title III, Information Security, December 17, 2002.

(2) P.L. 104-13, The Paperwork Reduction Act of 1995, as amended.

(3) OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Information Resources, dated February 8, 1996.

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

(1) NSTISSP No. 11, *National Information Assurance Acquisition Policy*, dated January 2000 (revised June 2003).

(2) NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, dated September 2002.

(3) NIST SP 800-46, Security for Telecommuting and Broadband Communications, dated September 2002.

(4) NIST SP 800-30, Risk Management Guide for Information Technology Systems, dated January 2002.

(5) NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, dated September 1996.

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

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

(2) DOE N 142.1, *Unclassified Foreign Visits and Assignments,* dated 7-14-99.

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

(4) DOE O 470.1, Change 1, *Safeguards and Security Program,* dated 09-28-95.

9. 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 205.11 IS APPLICABLE

Office of the Secretary
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 Electric Transmission and Distribution
Office of Energy Assurance
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 Safety Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Legacy Management
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
Office of Independent Oversight and Performance Assurance
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE N 205.11 *Security Requirements for Remote Access to DOE and Applicable Contractor Information Technology 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 flow down requirements to subcontractors unnecessarily or imprudently. 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.

1. REMOTE ACCESS. The contractor must use a documented risk-based approach to protect information and information systems consistent the principles and guidelines set forth in NIST SP 800-30, Risk Management Guide for Information Technology Systems, dated January 2002.

    a. The following applies to the contractor's remote access service.

    b. A documented risk-based approach must be used for information technology systems to determine the potential risk associated with system exposure to each user class identified in paragraph 1b(2)(b), below.

    c. Two principles apply.

        (1) Remote access is granted based on valid business and user need including scientific and other collaborative activities.

        (2) Least privilege is based on user classification (i.e., personnel remote access will be limited to the minimum privileges required by their user class).

            (a) General user accesses only general services on the system for which remote access is authorized.

(b) Privileged user has access to higher-level services (for example, system administration; special read, write, delete; or configuration change privileges) on the system for which remote access is authorized.

(c) Foreign national access is permitted as described in DOE N 205.2, *Foreign National Access to DOE Cyber Systems*, dated 11-01-99, or successor directives, and as detailed in the Departmental element's program cyber security plan (PCSP).

d. User IDs and passwords, as applicable, must be used. (See DOE N 205.3, *Password Generation, Protection, and Use*, dated 11-23-99, or successor directives.)

e. Clear-text, reusable passwords for remote access must not be used.

f. Security-enabled transmission capabilities must be implemented to the maximum extent possible.

g. Access will be granted only for authorized activities as identified within the Departmental element's PCSP provided to the contractor as described in the CRD to DOE O 205.1.

h. Contractors responsible for remote access systems, must provide continuous intrusion detection monitoring and must test the system at least annually to ensure continued adequate security, regardless of the specific controls implemented.

2. MINIMUM SECURITY CONTROLS. Below is a minimum set of management, technical, and operational controls. These minimum requirements apply to information systems that store or process DOE information or support DOE operations and assets.

e. Management Controls.

(1) Document automated tools (e.g., firewalls, virtual private networks, encryption, intrusion detection, anti-virus software, and audit log analysis) provided to manage remote access services.

(2) Document procedures to report and respond to remote access security incidents.

(3) Document procedures to conduct random security evaluation of remote access controls.

(4) Develop rules of behavior and the consequences for violations for all classes of users authorized remote access.

(5) Address specific security and awareness training for those authorized to use remote access services.

f. Operational Controls.

(1) Provide individuals with the minimum requirements for operating system and application software for personal equipment used for remote connection to DOE and contractor networks.

(2) Ensure that individuals granted remote access privileges commit to understanding and acknowledging the minimum requirements and the remote access rules of behavior.

(3) Ensure that risks associated with the potential use of split-tunneling or other external services are addressed and documented so that the appropriate controls are instituted and monitored for continued effectiveness.

g. Technical Controls.

(1) Document acceptable levels and types of authentication and personal identification for remote access.

(2) Document procedures to ensure that virus protection on remote equipment is included.

(3) Establish minimum requirements for the operating system and application software and for controlling and safeguarding government-issued cryptographic keying material on all equipment used for remote access.

(4) Describe the process for users to obtain approval from system and data owners prior to implementing remote network access.

(5) Document procedures to ensure updates of security software patches and/or hardware updates on remote equipment are included.

3. NATIONAL SECURITY SYSTEMS.[1]

Remote access to national security systems can be authorized when proper physical, personnel and cyber security controls are implemented at the host and remote sites and in a manner prescribed by DOE and national security directives. In particular, the contractor must use certified and accredited systems which use National Security Agency approved Type 1 encryption or information assurance enabled products conforming to policies set forth in NSTISSP 11.

[1] As defined in NIST SP 800-59 Guideline for Identifying an Information System as a National Security System, August 2003.

CONTRACTOR REQUIREMENTS DOCUMENT (CRD) APPLICABILITY

The Contractor Requirements Document for DOE N 205.11 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