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

NOTICE

DOE N 205.9

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

SUBJECT: CERTIFICATION AND ACCREDITATION PROCESS FOR INFORMATION SYSTEMS INCLUDING NATIONAL SECURITY SYSTEMS

1. OBJECTIVES.

   a. To establish Department of Energy (DOE) policy requirements and responsibilities for the certification and accreditation (C&A) of all DOE information systems including national security (classified) systems.

   b. To implement all applicable policies of the Office of Management and Budget (OMB) and national security authorities requiring C&A of DOE information systems.

   c. To implement the requirements 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.

   d. 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 (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 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).

DISTRIBUTION:
All DOE Organizations

INITIATED BY:
Office of the Chief Information Officer

(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 the contracts of affected site/facility management contractors via the laws, regulations, and DOE directives clause 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 the 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.

d. Exclusions. 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.

4. REQUIREMENTS.

All DOE information systems, which include national security systems, require C&A to ensure information and information systems are appropriately secure and operating at an

acceptable level of risk, thus reducing the potential impact to national and economic security. DOE's cyber security environment has many information systems, making C&A increasingly complex and difficult. This Notice provides DOE with a consistent process for ensuring the confidentiality, integrity, and availability of its information and information systems.

OMB Circular A-130, *Management of Federal Information Resources,* dated November 2000, requires Federal agencies to plan for security, ensure that appropriate officials are assigned security responsibility, and authorize system processing before starting operations and periodically thereafter. This authorization by senior Agency officials is referred to as accreditation. The technical and nontechnical evaluation of an information technology system produces the necessary information required by the approving official to make a credible, risk-based decision on whether to place the system into operation. This process is known as certification.

The C&A process is designed to certify that DOE information systems meet documented security requirements and will continue to maintain the accredited security posture throughout the system life cycle. The process allows DOE the flexibility to tailor the level of effort based on requirements for confidentiality, integrity, and availability. DOE information systems typically require basic security reviews, while national security systems require more comprehensive reviews. Confidentiality, integrity, and availability requirements will dictate the activities and tasks required for C&A.

C&A roles and responsibilities may be delegated. Heads of Primary DOE Organizations to which this directive is applicable (see Attachment 1) may appoint appropriate individuals, including contractors, to perform the activities associated with the certification process.

a. Implementation. Primary 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.

b. Certification and Accreditation. In implementing this Notice, DOE Organizations must use a documented C&A approach. The approach will be described in the applicable Program Cyber Security Plan (PCSP) and will be consistent with the principles and guidelines set forth in one or more of the following National Institute of Standards and Technology (NIST) publications.

(1) Federal Information Processing Standards Publication (FIPS PUB) 102, *Guideline for Computer Security Certification and Accreditation,* dated September 27, 1983, for Federal information systems.

(2) Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Second Public Draft),

dated June 30, 2003, scheduled to replace FIPS PUB 102 when it is finalized.

(3) SP 800-26, *Security Self-Assessment Guide for Information Technology Systems,* dated November 2001, may be used for system C&A provided applicable PCSPs permit such use and subject to the following conditions: (1) for low risk general support systems, a self-assessment meeting level three as set forth in SP 800-26 is conducted and (2) for medium or high risk general support systems or any major application, an independent review meeting level three as set forth in SP 800-26 is conducted.

c. General Requirements.

(1) All DOE information systems must be reaccredited every 3 years or when the operational, system, or technical characteristics have significantly changed. (C&A of national security systems is described in paragraph 5.)

(2) All DOE information systems must be covered by an approved security plan before accreditation can be granted.

(3) National security systems must have dedicated system security plans that comply with DOE M 471.2-2, *Classified Information Systems Security Manual,* dated 8-3-99.

(4) The designated approving authority must be a Federal employee.

d. Program Cyber Security Plan (PCSP) Requirements. The Primary DOE Organization's PCSP must establish and implement a C&A process for all national security systems, as described in paragraph 5, and will include the following.

(1) Roles and responsibilities of all key personnel responsible for the C&A of DOE information systems.

(2) Baseline security requirements (BLSRs) that address the appropriate levels of concern for confidentiality, integrity, and availability.

(3) Security test and evaluation (ST&E) requirements.

(4) Reporting process for the accreditation package.

(5) Specific training or support requirements for the C&A process.

(6) Documentation of all national security systems within the DOE Organization.

(7) Performance measures to indicate the level of implementation of C&A requirements across the Departmental suborganization.

e. Cyber Security Program Plan (CSPP) Requirements. Departmental suborganization CSPPs will include the following.

(1) Documentation that the implementation of the information system C&A process is consistent with the requirements of paragraph 4(b) and paragraph 5.

(2) Name and title of all DOE information systems controlled by the Departmental suborganization that require C&A.

(3) Levels of concern for the organization regarding confidentiality, integrity, and availability of its information systems.

(4) Management, operational, and technical controls for information systems (based on PCSP BLSRs).

(5) Roles and responsibilities for specific C&A activities such as ST&E.

f. Significant Changes. As described in DOE O 205.1 and OMB Circular A-130, Appendix III, significant changes 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) When introduction of new technologies or procedures causes a significant change in the level of risk, system-level security plans must be updated to reflect the increased risk and the risk mitigation techniques and methods to be used. Moreover, if introducing new technologies or processes increases the level of risk, it invalidates any existing authorization to process for that system or application (for example, certification and accreditation).

(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 operations or when significant changes occur.

(3) Primary DOE Organizations must be notified by system owners and operators of interconnected applications and systems of any 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.

(4) The Primary DOE Organization determines when a system must be reaccredited because of a significant change. Such determinations must be consistent with provisions of law, OMB policy, NIST guidance, and applicable DOE policies. DOE information systems must be reaccredited if a significant change occurs to the operational environment. Examples of significant changes include (a) changes to the level of concern for confidentiality, integrity, or availability; (b) hardware, software, or firmware additions, modifications, or upgrades requiring changes in the approved security controls; (c) significant threat changes; and (d) significant system configuration changes.

5. ADDITIONAL REQUIREMENTS FOR NATIONAL SECURITY SYSTEMS.[1]

All DOE national security systems must be certified and accredited in a manner consistent with the principles and guidelines in National Security Telecommunications and Information Systems Security Policy (NSTISSP) 6, the *National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems,* dated 4-8-94, and the *National Industrial Security Program Operating Manual* (NISPOM), dated 1995 (established pursuant to E.O. 12829, National Industrial Security Program, dated January 6, 1993). National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000, *National Information Assurance Certification and Accreditation Process (NIACAP)*, dated April 2000, provides guidance on how to implement NSTISSP 6. NISPOM Chapter 8 provides relevant processes for C&A. This guidance will be implemented using the procedures described in DOE M 471.2-2.

The guidelines for C&A of systems that process intelligence information are provided by the Director of Central Intelligence directives series of documents. The NISPOM supplement provides guidance for national security systems that process Special Access Program information, Sensitive Compartmented Information, or Restricted Data (RD) information.

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) Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information within Information Systems,* dated June 5, 1999.

[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.

(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) 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 2002.

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

(1) DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM)*,* dated January 1995.

(2) NIST FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation,* dated September 27, 1983.

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

(4) NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Second Public Draft), dated June 30, 2003.

(5) NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems,* dated November 2001.

(6) NSTISSI 1000, *National Information Assurance Certification and Accreditation Process (NIACAP)*, dated April 2000.

(7) NSTISSP 6, *National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems,* dated 4-8-94.

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

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

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

(3) DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy,* dated 5-8-01.

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 205.9 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 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
Secretary of Energy Advisory Board
Office of Independent Oversight and Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT
DOE N 205.9, *Certification and Accreditation Process for Information Systems and National Security 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.

1. CERTIFICATION AND ACCREDITATION (C&A). The contractor must use an approved C&A process to protect DOE information systems. Contractors must use one of the following C&A processes for unclassified systems.

   a. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication (PUB) 102, *Guideline for Computer Security Certification and Accreditation,* dated September 27, 1983.

   b. NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Second Public Draft), dated June 30, 2003, and scheduled to replace FIPS PUB 102 when finalized.

   c. NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems,* dated November 2001, may be used for system C&A provided the applicable Program Cyber Security Plan (PCSP) permits such use and subject to the following conditions: (1) for low risk general support systems, a self-assessment meeting level three (implementation of policies and procedures), as set forth in NIST SP 800-26, is conducted and (2) for medium or high risk general support systems or any major application, an independent review meeting level three, as set forth in NIST SP 800-26, is conducted.

2. NATIONAL SECURITY SYSTEMS. For national security systems, contractors must use National Security Telecommunications and Information Systems Security Instruction

(NSTISSI) 1000, *National Information Assurance Certification and Accreditation Process* (NIACAP), dated April 2000. NIACAP must be implemented with the relevant processes described in chapter 8 of the *National Industrial Security Program Operating Manual* (NISPOM), dated January 1995, and the procedures described in DOE M 471.2-2, *Classified Information Systems Security Manual,* dated 8-3-99. The C&A of national security systems that process intelligence information currently falls under the purview of the Director of Central Intelligence. The Director of Central Intelligence directives document series provides guidelines for C&A of these systems. The NISPOM supplement provides guidance for national security systems that process Special Access Program information, Sensitive Compartmented Information, or Restricted Data information. (Note: NIST SP 800-37 will supercede FIPS PUB 102 when finalized.)

3. MINIMUM REQUIREMENTS.

a. All DOE information systems must undergo reaccreditations every 3 years or when the operational, system, or technical characteristics have changed significantly.

b. All DOE information systems must be covered by an approved security plan before accreditation can be granted.

c. The self-assessment in NIST SP 800-26 must be completed annually for all DOE information systems. For low risk general support systems, a self-assessment using NIST SP 800-26 may also qualify as system certification pursuant to restrictions on this approach by the cognizant PCSP and provided the system meets level three as set forth in that publication. For medium or high risk general support systems or major applications, an independent review using NIST SP 800-26 may also qualify as system certification pursuant to restrictions on this approach by the cognizant PCSP and provided the system meets level three (i.e., implementation of policies and procedures) as set forth in that publication. The NIST SP 800-26 Self-Assessment must be completed annually for national security systems, but this will not meet the requirements of a system certification. C&A of national security systems must meet the requirements of paragraph 2 of this CRD.

d. The designated approving authority must be a Federal employee.

CONTRACTOR REQUIREMENTS DOCUMENT (CRD) APPLICABILITY

The CRD for DOE N 205.9, *Certification and Accreditation Process for Information Systems Including National Security Systems,* dated 2-19-04, 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

Accreditation. The formal declaration by a designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Certification. The comprehensive evaluation of the technical and nontechnical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Information System. An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

National Security System. Any information system (including any telecommunications system) used or operated by an Agency, by a contractor of an Agency, or by other organizations on behalf of an Agency. The function of the system (1) involves intelligence activities, (2) involves cryptologic activities related to national security, (3) involves command and control of military forces, (4) involves equipment that is integral to a weapon or weapons system, (5) is critical to the direct fulfillment of military or intelligence missions, or (6) is protected at all times by procedures established for information that has been specifically authorized under criteria established by an Executive order or by an act of Congress to be kept classified in the interest of national defense or foreign policy.