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

NOTICE

DOE N 205.10

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

SUBJECT: CYBER SECURITY REQUIREMENTS FOR RISK MANAGEMENT

1. OBJECTIVES.

   a. To establish Department of Energy (DOE) policy requirements and responsibilities for implementing a risk management approach to cyber security for all DOE information systems, including national security (classified) systems.

   b. To implement applicable policies of the Office of Management and Budget (OMB) and national security authorities requiring implementation of a risk management- and compliance-based approach to cyber security for national security 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 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.

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 any requirements of this Notice to other than site/facility management contractors will be communicated separately.

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

c. Exclusions. Consistent with 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. The purpose of risk management is to present a consistent life-cycle approach to managing risks to information and information systems in compliance with applicable laws, statutes, and guidance, including—

- OMB Circular A-130, *Management of Federal Information Resources,* dated November 2000, Appendix III, Security of Federal Automated Information Resources, and

- Public Law (P.L.) 107-347, The E-Government Act of 2002, Title III—Information Security [also known as the Federal Information Security Management Act (FISMA)], dated 12-17-02.

These statutes detail a full life-cycle, risk management approach that provides for a cost-effective, threat-based analysis and controls the implementation process.

National security systems must be protected according to guidelines of the *National Industrial Security Program Operating Manual (NISPOM)* (originally dated January 1995 and updated July 1997 and February 2001) and must implement procedures described in DOE M 471.2-2, *Classified Information Systems Security Manual,* dated 8-3-99.

FISMA also defines detailed responsibilities and activities to develop and maintain a full life-cycle, risk-based process for ensuring the secure operation of information systems and national security systems. FISMA §3544(a)(2), Federal Agency Responsibilities, requires the head of each Federal agency to ensure that senior Agency officials establish policies founded on a continuing risk management cycle that includes the need to—

- identify, assess, and understand risk;

- determine security needs commensurate with level of risk and magnitude of loss that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Agency;

- implement policies, procedures, and controls to adequately and cost effectively reduce risks to an acceptable level; and

- test and evaluate the effectiveness of security controls and practices periodically.

Risk management is composed of assessment, mitigation, and evaluation and assessment [paragraphs 4d(1)–(3), below]. Each requires a structured process for identifying, analyzing, and reducing the potential impact of risk events cost effectively. The structured process helps DOE staff understand their roles in and responsibilities for managing and containing risks associated with cyber security assets.

Risk management is applicable to systems regardless of their stage in the system life-cycle.

a. Implementation. Primary DOE Organizations must implement the requirements and meet the responsibilities defined in 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 Organization to all organizational levels.

b. General Requirements.

(1) A uniform risk management process permits managers to—

(a) effectively secure DOE general support systems (GSSs) and major applications (MAs);

(b) make informed risk management decisions and focus information technology expenditures on mitigating current risk factors;

(c) ensure interoperability and portability; and

(d) assist in understanding the total operational and residual risk.

(2) Management must implement a risk management approach to cyber security for unclassified systems to provide ongoing assurance that information systems are operating as planned under proposed security controls and that risk is maintained at an acceptable level and in a manner consistent with procedures and guidelines set forth in National Institute of Standards and Technology Special Publication (NIST SP) 800-12, *An Introduction to Computer Security: The NIST Handbook,* dated October 1995.

(3) Strong configuration management and system tests and evaluation must be documented and implemented to maintain acceptable levels of risk. A risk management approach for national security systems is outlined in paragraph 4d, below.

c. Determining Levels of Risk. The following requirements are based on law and OMB policy.

(1) As part of the risk management process, level of risk must be assessed for each system. Once identified, risk levels are used in selecting appropriate security controls to mitigate risk as described in the following paragraphs.

(2) Federal Information Processing Standard Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004, establishes a framework for determining levels of risk for each of the core security objectives for unclassified information systems:

- confidentiality,

- integrity, and
- availability.

(3) The risk levels as defined in FIPS PUB 199 and shown in Table 1, Categorization of Information and Information Systems, consider both impact and threat as prescribed by FISMA and provide guidance for selection, implementation, and ongoing operational assurance of security controls.

d. Risk Management. To manage risk for unclassified systems, Primary DOE Organizations must use a documented, cost-effective, risk-based approach consistent with procedures and guidelines set forth in NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* dated January 2002. This approach includes—

- identifying threats and vulnerabilities,
- documenting decisions on the adequacy and maintenance of security controls,
- determining cost implications of enhanced protection,
- accepting residual risk, and
- providing continuous monitoring of the system to ensure that controls are performing as required.

The major activities for conducting a risk management analysis, as detailed in NIST SP 800-30, are as follows.

(1) Risk Assessment. Identify and analyze (quantify) prospective events in terms of probability and consequences/impacts. The following are required elements of risk assessment.

(a) Identify and describe each organizational GSS and MA.

(b) Assess threats, vulnerabilities, likelihood of adverse actions, and potential consequences.

(c) Evaluate security control options and their impacts on risk posture.

(d) Develop from findings of those analyses [paragraphs 4d(2)(a)-(c)] a set of security controls.

(e) Document decisions made during the assessment.

Table 1. Categorization of Information and Information Systems.[1]

	LEVEL OF RISK		
SECURITY OBJECTIVE	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on Agency/site/facility operations (including mission, functions, image or reputation), Agency assets, or individuals. A loss of confidentiality could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on Agency/site/facility operations (including mission, functions, image or reputation), Agency/site/facility assets, or individuals. A loss of confidentiality could be expected to cause **significant degradation in mission capability, place the Agency at a significant disadvantage**, or result in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic** adverse effect on Agency/site/facility operations (including mission, functions, image or reputation), Agency assets, or individuals. A loss of confidentiality could be expected to cause **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
Integrity Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on Agency/site/facility operations (including mission, functions, image or reputation), Agency assets, or individuals. A loss of integrity could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on Agency/site/facility operations (including mission, functions, image or reputation), Agency/site/facility assets, or individuals. A loss of integrity could be expected to cause **significant degradation in mission capability, place the Agency/site/facility at a significant disadvantage,** or result in **major** damage to assets**,** requiring **extensive** corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **severe** or **catastrophic** adverse effect on Agency/site/facility operations, (including mission, functions, image or reputation), Agency/site/facility assets, or individuals. A loss of integrity could be expected to cause **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on Agency/site/facility operations (including mission, functions, image or reputation), Agency/site/facility assets, or individuals. A loss of availability could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on Agency/site/facility operations (including mission, functions, image or reputation), Agency/site/facility assets, or individuals. A loss of availability could be expected to cause **significant degradation in mission capability, place the Agency at a significant disadvantage**, or result in **major** damage to assets, requiring **extensive** corrective actions or repairs.	The disruption of access to or use of information or an information system could be expected to have a **severe** or **catastrophic** adverse effect on Agency/site/facility operations (including mission, functions, image or reputation), Agency/site/facility assets, or individuals. A loss of availability could be expected to cause **a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets**.

[1] Table taken from National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (May 2003 draft). Applies only to unclassified information systems.

(2) Risk Mitigation. Documented findings from the risk assessment are used as input for the mitigation process. To complete the risk mitigation function, the following actions are required. Use the risk assessment to prioritize actions that will most likely result in maximum risk reduction.

(a) Evaluate recommended security controls and select those that provide the greatest level of risk reduction at the lowest cost.

(b) Identify appropriate security controls and assign responsibility to those individuals who will implement and maintain those controls.

(c) Implement security controls and document the implementation to provide input to the configuration baseline.

(3) Evaluation and Assessment. Evaluate risk reduction achieved and continuously monitor the systems to ensure that security controls are functioning as expected. Activities to accomplish this evaluation and to create a feedback process to verify the results of risk assessment and mitigation include verifying that—

(a) the first two phases are properly documented and reflected in the GSS baseline;

(b) security controls have been or are being implemented;

(c) recurring accreditation processes are in place to track the system and schedule appropriate testing and evaluation activities;

(d) employees understand their responsibilities; and

(e) appropriate awareness and training functions are set up properly.

e. Program Cyber Security Plan Requirements. The following will be documented in the plan, as required by DOE O 205.1.

(1) Roles and responsibilities of key personnel who incorporate risk management concepts and principles into the environment.

(2) Process that will be used to conduct risk management, including risk assessments, risk mitigation, and evaluation and assessment. (NOTE: If the Primary DOE Organization is not using the NIST SP 800-30 process, the replacement process should be described in sufficient detail to show that it is functionally equivalent.)

(3) Capital planning issues related to integrating risk management policies into the environment, including incorporating and funding risk-based

security controls over the life cycle of individual systems, as required by law.

(4) Minimum security controls that are to be expected or enforced based on the level of risk for information systems.

(5) Performance measures to indicate the level of risk management requirements implementation across the Primary DOE Organization.

f. Cyber Security Program Plan Requirements. The following will be documented in the plan, as required by DOE O 205.1.

(1) Roles and responsibilities of key personnel responsible for risk management strategy, implementation, and maintenance for DOE networks or devices.

(2) Specific processes that will be used to complete risk assessment, risk mitigation, and evaluation and assessment functions as detailed in NIST SP 800-30. (NOTE: Exceptions for specific operating environments are to be highlighted, and identification of a functionally equivalent alternative process will be provided.)

(3) Specific technical, operational, and management security controls necessary to provide assurance that risk is maintained at an acceptable level. (NOTE: Security controls must be tested to ensure that they continue to operate as intended.)

(4) Specific training or support requirements to ensure that personnel understand and support security controls. (NOTE: Training must include individual rules of behavior and consequences for rules violation.)

g. Significant Changes.

(1) 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.

(2) 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.

(3) 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.

(4) 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. DOE M 471.2-2 requires that a security plan be developed and maintained in coordination with the site security plan or a site safeguards and security plan. These documents establish the level of security required before system development begins or when changes are made to the system.

(1) System changes that might require design changes or that could alter the system's risk profile must be documented and reported to the organization's designated approving authority.

(2) Prudent risk reduction controls must be implemented and documented to provide assurance that the national security system is operating as intended in the security plan.

b. E.O. 12829, National Industrial Security Program, dated January 6, 1993, directed the development of *NISPOM* [Department of Defense 5220.22-M]. Chapter 8 of *NISPOM* includes guidance on requirements, restrictions, and safeguards to prevent unauthorized disclosure and control authorized disclosure of classified information created, stored, or processed on national security systems.

6. RESPONSIBILITIES.

a. Secretary of Energy develops, documents, and implements a DOE-wide program to provide security for the information and information systems that support DOE operations and assets.

b. Office of the Chief Information Officer.

(1) Is responsible for development and maintenance of cyber security policies, Orders, Manuals, and guidelines, including risk management

requirements documented in existing DOE policies as required by DOE O 205.1.

(2) Provides strategic direction and guidance for the Department's risk-based process to ensure cyber security for DOE information and national security systems.

(3) Evaluates, monitors, and reports on performance of the risk management process to senior DOE management.

(4) Monitors planning, budgeting, and expenditures for risk management and coordinates with other cyber security initiatives for efficiency and cost-effectiveness.

(5) Coordinates with the Office of Security to ensure a consistent approach to protecting DOE information assets.

c. <u>Office of Security</u>.

(1) Coordinates with the OCIO on cyber security risk management issues.

(2) Coordinates with OCIO to enable a consistent approach to protecting DOE information assets.

(3) Develops and maintains DOE noncyber security policies for protecting classified information.

d. <u>Heads of Primary DOE Organizations</u> (see Attachment 1). Note that except for item (1) below, authority for these actions may be reassigned.

(1) Assume accountability for risk management and accept overall residual risk throughout their organizations.

(2) Implement the risk management process for their organizations consistent with directives and guidance from the OCIO.

(3) Designate single points of contact to represent their organizations to OCIO and the cognizant security agency (CSA) on risk management issues.

(4) Notify contracting officers when contractors under their purview are affected by DOE cyber security directives.

(5) Designate single points of contact to represent their organizations on risk management issues and to whom day-to-day risk management activities may be delegated. [NOTE: While authority for ensuring the risk management process, including any or all of the responsibilities in

paragraphs 5e(5)–(13) may be delegated, accountability remains with the Head of the Primary DOE Organization.]

(6) Identify threats to and vulnerabilities of DOE information and national security systems under their cognizance.

(7) Coordinate the development and implementation of a risk management approach to cyber security in their organizations and in contracts under their cognizance.

(8) Ensure that risk levels for national security systems under their control are met and maintained.

(9) Develop and maintain system security authorization agreements (SSAAs) for national security systems.

(10) Implement and document risk reduction controls to provide assurance that national security systems under their control are operating as intended in the SSAAs.

(11) Determine the cost implications of implementing the risk management process and ensure that adequate funds are available and security costs are integrated into overall system costs.

(12) Keep cognizant Primary DOE Organizations informed of risk management issues that need senior management attention.

(13) Oversee contractor compliance with requirements of this Notice.

(14) Maintain complete documentation on management, technical or operational control decisions to mitigate threats to system vulnerabilities.

(15) Provide ready access to facilities for CSA and other risk management surveys.

(16) Respond to CSA recommendations.

(17) Develop annual reports on risk management and other such reports as may be required.

e. <u>Designated Cyber Security Risk Management Points of Contact</u> represent their organizations on risk management issues and perform other day-to-day risk management activities delegated to them.

f. <u>Information System Administrators</u> coordinate with organization risk management points of contact to ensure a cohesive risk management process and documentation of system changes.

g. Contracting Officers, once advised by their Lead Program Secretarial Officers, incorporate the CRD of this Notice into affected contracts.

7. DEFINITIONS. Terms relevant to this Notice are defined in Attachment 4.

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) P.L. 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.

(2) E.O. 12958, *Classified National Security Information*, dated April 17, 1995.

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

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

(5) E.O. 12829, *National Industrial Security Program*, dated January 6, 1993.

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

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

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

(1) NIST FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.

(2) National Security Telecommunications and Information Systems Security Instruction 1000, *National Information Assurance Certification and Accreditation Process (NIACAP)*, dated April 2000.

(3) Department of Defense 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, dated January 1995 (with July 1997 and February 2001 changes).

(4) NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, dated October 1995.

(5) NIST SP 800-30, Risk Management Guide for Information Technology Systems, dated October 2001.

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

9. CONTACT. Questions concerning this Notice should be directed to the Chief Information Officer's 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 205.10 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 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
Secretary of Energy Advisory Board
Office of Legacy Management
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT
DOE N 205.10, *CYBER SECURITY REQUIREMENTS FOR RISK MANAGEMENT*

This Contractor Requirements Document (CRD) establishes requirements for Department of Energy (DOE) and National Nuclear Security Administration contractors with access to DOE information systems.

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.

This CRD supplements requirements contained in the CRD (Attachment 2) 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. The contractor will ensure that it and its subcontractors cost effectively comply with the requirements of this CRD.

1. INFORMATION SYSTEMS. For DOE information systems, the contractor must use a risk management approach consistent with the principles and guidelines of National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems, dated October 2001, for protecting information and information systems. A documented risk management process must be used to support informed decisions on the adequacy of protection, cost implications of further enhanced protection, and the acceptance of residual risk.

2. NATIONAL SECURITY SYSTEMS. For national security systems, the contractor must meet requirements of Executive Order 12829, which established the National Industrial Security Program and directed the development of the Department of Defense (DoD) 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, dated January 1995. Chapter 8 of *NISPOM* sets forth requirements, restrictions, and other safeguards to prevent unauthorized disclosure and control authorized disclosure of classified information created, stored or processed on national security information systems.

   The CRD (Attachment 2) of DOE M 471.2-2 *Classified Information Systems Security Manual*, dated 8-3-99 provides guidance for implementing requirements of DoD 5220.22-M to ensure the security of DOE national security systems.

CONTRACTOR REQUIREMENTS DOCUMENT (CRD) APPLICABILITY

The CRD for DOE N 205.10 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

Accountability. The security goal that requires the actions of an entity to be traceable uniquely to that entity. Accountability supports nonrepudiation, deterrence, fault isolation, intrusion detection, prevention, and after-action recovery and legal action.

Assurance. In the context of cyber security, assurance is confidence that security goals (integrity, availability, confidentiality, and accountability) have been met adequately by specific implementation of security plans. Security goals are *adequately* met when—

- functionality performs correctly,
- sufficient protection against unintentional errors (by users or software) is in place, and
- sufficient resistance to intentional penetration or bypass exists.

Availability. The security goal that generates requirements for protection against—

- unauthorized, intentional or accidental attempts to delete data or otherwise cause a denial of service or data and
- unauthorized use of system resources.

Cognizant Security Agency (CSA). Agencies of the executive branch authorized by Executive order to establish industrial security programs to safeguarding classified information under the jurisdiction of Federal agencies when disclosed or released to U.S. industry. See the *National Industrial Security Program Operating Manual (NISPOM),* dated January 1995, for complete discussion/limitations on CSAs.

Confidentiality. The security goal that requires protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, being processed, and in transit.

Cyber Security Program Plan. Part of the Primary DOE Organization cyber security program that provides specific information on planning, budgeting, implementing, operating, and maintaining cyber resources to fulfill the program Secretarial Officer cyber security plan and the DOE Cyber Security Management Program.

Departmental Subelements. Remote offices and entities reporting to heads of Primary DOE Organizations.

General Support System. An interconnected set of information resources under the same direct management control which share common functionality. Includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support various mission-related functions. Users may be from one or several organizations.

Information System or Information Technology System. The set of Agency information resources organized for collecting, storing, processing, maintaining, using, sharing, disseminating, disposing, displaying, or transmitting information. Information technology systems are categorized as either major applications or general support systems.

Integrity. A security condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Major Application (MA). An application that requires special attention to security because of the risk and magnitude of harm that could result from loss, misuse, or modification of information or unauthorized access to information in the application. A breach in an MA might compromise many individual application programs and hardware, software, and telecommunications components. MAs can be major software applications or a combination of hardware and software where the only purpose of the system is to support a specific mission-related function.

Primary DOE Organizations: Refer to those listed in Attachment 1.

Program Cyber Security Plan. An outline of how a DOE program Secretarial Office or administration office plans to implement and maintain cyber security for the cyber assets/resources under its purview.

Security Controls. Management, operational, and technical measures prescribed for an information technology system which, taken together, satisfy specified security requirements and protect the confidentiality, integrity, and availability of the system and its information. Security controls can be selected from a variety of families including risk management, system development and acquisition, configuration management, system interconnection, personnel security, media protection, physical and environmental protection, contingency planning, incident response capability, hardware and system software maintenance, system and data integrity, and security awareness and training and education documentation, identification, and authentication; logical access; audit; and communications.

Threat. Potential for a threat-source to either accidentally trigger or intentionally exploit a specific vulnerability.

Vulnerability. A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of system security policy.