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

ORDER

DOE O 205.1

Approved: 3-21-03
Sunset Review: 3-21-05
Expires: 3-21-07

SUBJECT: DEPARTMENT OF ENERGY CYBER SECURITY MANAGEMENT PROGRAM

1. OBJECTIVES. The purpose of the Department of Energy (DOE) Cyber Security Management Program (hereafter called the Program) is to protect all DOE cyber information and information systems in order to implement the requirements of applicable laws required to maintain national security and ensure DOE business operations proceed without security events such as interruption or compromise. Protection must be provided using a mission-compatible, cost-effective risk management process that applies appropriate measures to ensure the confidentiality, integrity, and availability of cyber information and information systems. Cyber security management must be integrated into management and work practices at all levels so that all personnel are responsible for protecting cyber assets under their control. This Order has the following objectives.

   a. To establish a Program that integrates cyber security into management and work practices at all levels in the Department according to DOE cyber security management policy contained in DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01. The Cyber Security Management Plan (CSMP) is the cyber security element of the Integrated Safeguards and Security Management (ISSM) Program.

   b. To protect DOE cyber systems and general support systems, commensurate with the risks they face and the magnitude of harm that could result from the loss, misuse, disclosure, or unauthorized modification of information entered, processed, stored, displayed, or transmitted on/with them.

   c. To establish requirements and assign responsibilities for protecting all DOE controlled cyber information and information systems (classified and unclassified).

   d. To establish an agile CSMP that addresses rapidly changing threats, vulnerabilities, missions, and technologies.

   e. To achieve and maintain cyber security competencies throughout the DOE Federal and contractor workforce sufficient to enable personnel to fulfill their responsibilities in protecting the Department's cyber information and information systems.

f. To provide for continuous improvement of cyber security.

g. To describe the DOE managerial structure that will support implementing Office of Management and Budget, Circular A-130, Appendix III.

2. CANCELLATIONS. DOE N 205.1, *Unclassified Cyber Security Program*, dated 7-26-99. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with such a directive. Cancelled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the cancelled directives.

3. APPLICABILITY.

a. DOE Elements. Except for the exclusions in paragraph 3c, this Order applies to the DOE programs, elements, and administrations listed in Attachment 1.

b. Site/Facility Management Contracts. The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Order that will apply to site/facility management contracts that include the CRD.

This CRD must be included in site/facilities management contracts that provide access to DOE cyber systems.

This Order does not automatically apply to other than site/facility management contracts. Any application of any requirements of this Order to other than site/facility management contracts will be communicated separately from this Order.

Attachment 3 contains definitions relevant to this Order.

The official identified in the Responsibilities paragraph is responsible for notifying the contracting office of which site/facility management contracts are affected. Once notified, the contracting officer is responsible for incorporating the CRD into each affected site/facility management contract via the Laws, regulations and DOE directives clause of the contract.

The site/facility contractors to which this CRD applies are contained in Attachment 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. 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.

c. Exclusions. Consistent with the responsibilities identified in Executive Order 12344, and as detailed in Section 5, Responsibilities, the Director of the Naval Nuclear Propulsion Program will ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, and implement and oversee all requirements and practices pertaining to this DOE Order for activities under the Deputy Administrator's cognizance.

4. REQUIREMENTS. DOE cyber assets must be protected in compliance with the requirements of applicable national laws, which require DOE to provide information security protection commensurate with their importance to DOE missions and programs, their importance to national security, their vulnerability to threats, and the magnitude of harm that would result from compromise of those assets. This Order establishes the following requirements:

a. Risk Management. DOE elements must use a documented risk-based approach, in accordance with a Program Cyber Security Plan (PCSP), to make informed decisions for protecting cyber assets under their purview, including decisions on the adequacy and maintenance of protection, cost implications of enhanced protection, and acceptance of residual risk by heads of DOE elements.

b. Implementation. The CSMP must be implemented at all organizational levels. Requirements and responsibilities will flow down, as appropriate, from the heads of DOE elements to all subordinate organizational levels.

c. Program Direction. The cognizant Lead Program Secretarial Offices (LPSOs) will issue direction on cyber security matters to multi-site programs. Such matters must be coordinated with other DOE elements that are responsible for cyber information or information systems at the LPSO managed site.

d. Cyber Security Plan Development and Maintenance. PCSPs, Cyber Security Program Plans (CSPPs) and their associated Security Plans must be developed, approved, and maintained in accordance with applicable directives. PCSPs and CSPPs, must be reviewed in accordance with the Federal Information System Management Act (FISMA) and updated as needed when operational considerations (e.g., risks, threats, general support system configurations, vulnerabilities, or DOE cyber security directives) change significantly, but not less frequently than every 2 years. Security Plans and CSPPs that function as Security Plans must be completed annually. Heads of DOE elements will maintain approved copies of PCSPs and CSPPs for audit and monitoring purposes with the ability to provide copies of the plans and referenced supporting material to authorized requestors within 2 business days from the date of request.

e. Program Cyber Security Plans. Heads of DOE elements and the DOE Chief Information Officer (CIO) must develop and maintain PCSPs. PCSPs must address—

(1) roles and responsibilities, including reporting incidents of security concern;

(2) organizational structure;

(3) cyber asset operating environments;

(4) protection of cyber resources;

(5) planning and budget (including personnel resources);

(6) applicable standards (both national and DOE);

(7) graded information protection;

(8) risk management, including use of—

(a) wireless and personal electronic devices,

(b) remote access, and

(c) baseline security requirements;

(9) certification and accreditation;

(10) security, testing, and evaluation;

(11) configuration management;

(12) monitoring and auditing (including review, tracking, structure of corrective action plans);

(13) strategy for continuity of operations;

(14) cyber security program performance-based management, including metrics;

(15) cyber security program education, training, competencies, and awareness;

(16) performance evaluation; and

(17) incident reporting and response.

f. Cyber Security Program Plans. Each DOE organization, as defined in any PCSP, that owns, uses, maintains or accesses cyber information or information systems must develop, implement, and maintain a CSPP for protecting these cyber information and cyber assets or other cyber information and information systems that are considered Critical Infrastructure Protection (CIP) assets by the heads of DOE elements or the DOE CIO. The CSPPs must address—

(1) system environment;

(2) roles and responsibilities, including reporting incidents of security concern;

(3) information systems and their interfaces;

(4) configuration management;

(5) incident, warning, and advisory response;

(6) cyber security controls;

(7) threat, risk, and vulnerability posture, including cyber perimeter protection techniques and baseline security requirements;

(8) cyber security program education, training, competencies, and awareness;

(9) performance evaluation and self-assessment;

(10) plan change management; and

(11) resource requirements.

g. Implementation Schedule. DOE elements and administrations must implement this Order within 180 days after its issuance. Extensions to the 180-day limit will be determined on a case-by-case basis by the Office of the CIO (OCIO).

h. Compliance. All cyber activities must comply with the requirements of and achieve the objectives of applicable laws, regulations, Executive orders, national directives, and DOE directives, including DOE and national directives for handling classified or special access matter.

5. RESPONSIBILITIES.

a. Office of the Chief Information Officer.

(1) Develops and maintains Departmental cyber security policies, Orders, Manuals, and guidelines. This will be accomplished by, but not limited to—

(a) providing strategic direction for managing remote access to DOE information systems;

(b) establishing certification and accreditation requirements for DOE, incorporating applicable national policy and standards, for approving all classified and unclassified information systems covered by the CSMP;

(c) developing and maintaining PCSP and CSPP requirements and guidance;

(d) establishing and managing an Independent Verification & Validation (IV&V) program;

(e) evaluating and monitoring the performance of the Program by analyzing PCSP and CSPP reviews, oversight reports, results of peer reviews, and other applicable performance-based metrics and

measures and reporting on program performance to senior DOE management; and

(f) providing direction and guidance as applicable for managing non-U.S. citizen access to and use of DOE cyber assets (specifically including privileged access and access for non-U.S. citizens from sensitive countries).

(2) Coordinates the Department's response to the reporting and program review requirements of FISMA.

(3) Monitors planning for and expenditures of DOE cyber security resources by coordinating with the Chief Financial Officer on the Department's cyber security budget and on supporting the Department's information technology capital planning processes.

(4) Manages Department-wide central cyber incident reporting and response activities in coordination with the Office of Security, Office of Counterintelligence, Office of Inspector General, and other DOE elements, as circumstances warrant.

(5) Directs Computer Incident Advisory Capability (CIAC) support in providing watch and warning capabilities, analysis, and assistance reviews.

(6) Participates in Office of Independent Oversight and Performance Assurance assessments, and reviews findings and recommends responsive actions for improving the CSMP.

(7) Develops and maintains a process for documenting and monitoring the correction of significant cyber security deficiencies in DOE.

(8) Establishes and manages a cyber security education, training, and awareness program, including roles and responsibilities for responding to incidents and reporting incidents of security concern.

(9) Maintains the OCIO Cyber Security Policy Working Group and chairs the cyber security advisory panel.

(10) Serves as the Department's primary point of contact for cyber security issues with other Federal Agencies.

(11) Implements the CSMP for all cyber information and information systems at DOE Headquarters. In this capacity, fulfills Program Secretarial Officer (PSO) responsibilities for DOE Headquarters cyber assets.

(12) Establishes policy and guidance as applicable for Department-wide communications security (COMSEC) and TEMPEST, including—

(a) accountability for all COMSEC materials by serving as the manager of the DOE COMSEC Central Office of Record and

(b) countermeasures based on a risk management approach by serving as the DOE certified TEMPEST technical authority.

(13) Establishes appropriate policy and guidance for Public Key Infrastructure (PKI) in support of DOE missions and business processes and implements the PKI program for Department-wide communications security.

In carrying out these responsibilities, guidance rendered by the CIO with respect to components of the National Nuclear Security Administration (NNSA) shall be provided to the Administrator, NNSA, for appropriate action. The CIO and NNSA will be expected to coordinate anticipated NNSA actions pursuant to this Order.

b. Office of Security.

(1) Coordinates with the OCIO to provide input in the development of cyber policies to ensure a consistent approach in protecting the Department's information assets.

(2) Manages Department-wide central Incidents of Security Concern Reporting Program in accordance with DOE N 471.3 *Reporting Incidents of Security Concern,* dated 4-13-01 and its successors.

(3) Coordinates with Office of Independent Oversight and Performance Assurance program activities, as appropriate, and reviews findings for security policy issues.

c. Heads of Departmental Elements.

(1) Assume accountability for cyber security and accept the overall residual risk throughout their organizations. (Although the authority and responsibility for accepting residual risk may be delegated, the accountability for ensuring that cyber information and information systems are protected and risk is being appropriately managed remains with the head of the Departmental element.) These individuals are ultimately the Designated Approving Authorities (DAAs) for their respective programs/administrations.

(2) Ensure that system Certification and Accreditation (C&A) activities are performed.

(3) Ensure and document processes for reviewing and approving all CSPPs.

(4) Notify the appropriate contracting officers, ensure that the CRD is incorporated into relevant contracts, and provide program direction to implement requirements of the PCSP and CSPPs.

(5) Ensure that all CIP assets are listed in CSPPs.

(6) Designate formally individuals who will be the focal points for cyber security within their Departmental elements. (Even though authority for ensuring effective cyber security may be delegated, accountability remains with the head of the Departmental element.) This Departmental element focal point for cyber security will—

(a) establish, implement, document, and maintain a PCSP that implements the Program;

(b) identify in coordination with the OCIO, cyber assets that require a separate CSPP (e.g., major systems that have significant risk or that reside in multiple DOE organizations or multiple LPSOs);

(c) facilitate external and internal reviews, including those involving DOE independent oversight;

(d) coordinate with the OCIO in evaluating the performance of the cyber security program;

(e) ensure that sufficient resources are identified, planned, and requested to implement and maintain the PCSP;

(f) monitor the effectiveness of the PCSP implementation through program reviews, self-assessments, management assessments, performance metrics analyses, peer reviews, and vulnerability analyses; and

(g) report PCSP implementation performance to the OCIO using PCSP and OCIO-established cyber security and performance metrics.

(7) Ensure the appointment of individuals to be the focal points for cyber security in each of a DOE element's subsidiary organizations. Each of those appointed individuals will—

(a) establish, implement, document, and maintain a CSPP that implements the PCSP;

(b) ensure the CSPP describes the process and timeline for integrating and implementing PCSP cyber security requirements throughout the organization;

(c) ensure that the CSPP includes or references an implementation plan or set of procedures;

(d) ensure that cyber assets owned by other entities but under the stewardship of the organization are addressed in the organization's CSPP;

(e) coordinate with the DOE element in monitoring the cyber security program;

(f) ensure that sufficient resources are identified, planned, requested, allocated, and applied to implement and maintain the CSPP; and

(g) monitor the effectiveness of the CSPP implementation through program reviews, self-assessments, management assessments, DOE element performance metrics, peer reviews, and vulnerability analyses.

d. Chief Financial Officer. Coordinates cyber security budgets and funding with the heads of DOE elements and the OCIO, as appropriate.

e. The Office of Independent Oversight and Performance Assurance.

(1) Establishes and implements an independent oversight program for Program implementation and compliance in accordance with DOE O 470.2B, *Independent Oversight and Performance Assurance Program*, dated 10-31-02.

(2) Implements an independent oversight program for evaluating Program performance and compliance encompassing all DOE elements.

(3) Implements an independent oversight program for evaluating PCSP performance and compliance encompassing all DOE elements.

(4) Conducts performance testing, including external network penetration testing, as part of cyber security inspections to evaluate the effectiveness of cyber security measures.

(5) Provides feedback to Headquarters organizations on the effectiveness of DOE cyber security policy and implementation, and recommends improvements for cyber security programs to the heads of DOE elements, the Office of Security, and the OCIO.

(6) Conducts the annual evaluation of classified cyber security for the Department in accordance with the Federal Information Security Management Act of 2002 and related legislation. Also provides input to

the Office of Inspector General for the annual evaluation of unclassified cyber security programs.

(7) Coordinates with the OCIO and Office of Counterintelligence on topics of concern for scheduled inspections.

(8) Notifies the OCIO, Office of Counterintelligence, Office of Security, and heads of DOE elements of scheduled inspections and provides opportunities to participate.

f. Office of Counterintelligence. The Office of Counterintelligence's cyber programs are designed to detect, deter, investigate, exploit, and neutralize technical intelligence activities, espionage, sabotage, and international terrorist activities directed against DOE cyber assets. The Information and Special Technologies Directorate within the Office of Counterintelligence will provide counterintelligence (CI) services to DOE in accordance with CI directives. Such services include coordinating investigations, disseminating threat information, and relevant technical information from U.S. intelligence community resources.

(1) Acts as primary liaison with the intelligence community on CI and technical vulnerability issues.

(2) Provides relevant threat information, including a classified threat statement for the Department, to the Office of Security, the OCIO, and other DOE elements to assist in the development, improvement, and maintenance of the CSMP.

g. Director of Intelligence.

(1) Serves as the DAA for classified cyber assets in DOE that process intelligence information. When intelligence information is on the same system as other DOE information assets, provides the results of the Certification &Accreditation (C&A) to cognizant DOE elements for review.

(2) Interprets and implements Central Intelligence Agency (CIA) directives governing the processing of intelligence information.

(3) Coordinates with the CIA to ensure that an independent, performance-based assessment of all relevant intelligence cyber assets is performed every 3 years in accordance with CIA directives and that the results are furnished to the Secretary of Energy.

(4) Coordinates with the Office of Counterintelligence to provide relevant threat information, including a classified threat statement for the Department, to the Office of Security, the OCIO, and other DOE elements to assist in the development, improvement, and maintenance of the CSMP.

h. Office of Inspector General.

(1) Coordinates investigative issues concerning the CSMP and other cyber security efforts with the Office of Security, the OCIO, the Office of Counterintelligence staff, and other DOE elements.

(2) Conducts investigations of intrusions and anomalous activity in Departmental cyber information and information systems.

(3) Coordinates investigative activity with the Office of Security, the OCIO, and other Departmental organizations and law enforcement agencies as required.

(4) Provides relevant criminal threat information to the Office of Security, the OCIO and other DOE elements to assist in the development, improvement, and maintenance of the CSMP.

(5) Is responsible for collecting input for and producing the annual evaluation of unclassified cyber security programs.

6. REFERENCES.

a. The following DOE directives contain relevant requirements, standards, and procedures for the CSMP.

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

(2) DOE G 205.1-1, *Cyber Security Architecture Guidelines*, dated 03-08-01.

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

(4) DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.

(5) DOE N 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents,* dated 3-18-02.

(6) DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 3-22-01.

(7) DOE O 221.2, *Cooperation with the Office of Inspector General*, dated 3-22-01.

(8) DOE N 221.8, *Reporting Fraud, Waste, and Abuse,* dated 7-29-02.

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

(10) DOE O 470.2B, *Independent Oversight and Performance Assurance Program,* dated 10-31-02.

(11) DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information,* dated 6-30-00.

(12) DOE N 471.3, *Reporting Incidents of Security Concern,* dated 4-13-01.

(13) DOE 5670.3, *Counterintelligence Program,* dated 9-04-92.

b. The following non-DOE documents contain cyber security program references.

(1) Atomic Energy Act of 1954 as amended by the Energy Reorganization Act of 1974.

(2) The Paperwork Reduction Act of 1995.

(3) Information Technology Management Reform Act of 1996, also known as the Clinger-Cohen Act of 1996.

(4) E-Government Act of 2002 (P.L. 107-347), Title III, Information Security.

(5) EO 13231, "Critical Infrastructure Protection in the Information Age," dated 10-16-01.

(6) EO 13010, "Critical Infrastructure Protection," dated 7-15-96.

(7) EO 13011, "Federal Information Technology," dated 7-17-96.

(8) EO 12344, "Naval Nuclear Propulsion Program," dated 2-1-82.

(9) EO 12958 "Classified National Security Information," dated 4-17-95.

(10) National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems.

(11) Office of Management and Budget Circular A-130, *Management of Federal Information Resources,* dated November 2000.

7. CONTACT. Questions concerning this Order should be directed to the CIO's Office of Cyber Security, at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

DOE ORGANIZATIONS TO WHICH DOE O 205.1 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 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 Independent Oversight 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 Security
Office of Worker and Community Transition
Office of Energy Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE O 205.1, *DEPARTMENT OF ENERGY CYBER SECURITY MANAGEMENT PROGRAM*

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

1. CYBER RESOURCE PROTECTION. The contractor must protect all DOE unclassified and classified information and information systems under its management and control at all times commensurate with the risk and magnitude of harm that could result to national security interests and DOE missions and programs resulting from a loss of confidentiality, availability, integrity of these information or systems.

2. RISK MANAGEMENT. The contractor must use a risk management approach in protecting information and information systems. A documented risk management process, described further in paragraph 3 below, must be used to support informed decisions related to the adequacy of protection, cost implications of further enhanced protection, and the acceptance of residual risk.

3. PROGRAM EVALUATION AND CYBER SECURITY PLAN DEVELOPMENT AND MAINTENANCE. Contractors' Cyber Security Program Plans (CSPPs) must be developed, approved, and maintained in accordance with the applicable DOE element's Program Cyber Security Plan (PCSP). The PCSP will be provided to the contractor by a site management official who will be the designated point of contact. The contractor's plans must be reviewed and updated by the contractor as needed when operational considerations (e.g., risks, threats, cyber asset configurations, vulnerabilities, or DOE cyber security directives) change significantly, but not less than every 2 years. Security Plans and CSPPs that function as Security Plans must be completed annually.

4. EXAMPLES. The following are examples of requirements which may be placed on the contractor and arise out of requirements contained in the DOE element PCSP.

   a. CSPP Assessment and Review. The contractor must support and fulfill cyber security performance assessment approaches identified in DOE cyber security directives and PCSPs as appropriate. To ensure that the CSPP is properly implemented, the contractor must ensure that it does the following.

      (1) Performs not less than every year, an organizational and system self-assessment in a manner that meets or exceeds self-assessment

guidance. To permit accurate DOE reporting to the Office of Management and Budget, the results of self-assessments must be provided to the site point of contact.

(2) Arranges for a peer organization review at least every 3 years. Such review must assess the contractor's conformance with the approved contractor's CSPP. The results must be provided to the site Point of Contact.

b. Corrective Action Plans. The contractor must develop and maintain procedures, in accordance with the DOE element's PCSP, for identifying, documenting, correcting, and reporting significant cyber security deficiencies in DOE cyber assets under their span of control.

c. Security Monitoring. The contractor in accordance with the procedures outlined in the DOE element PCSP must make timely reports of security incidents to the site incident response team and/or the Computer Incident Advisory Capability (CIAC) as appropriate. The contractor must provide cyber security coverage in accordance with the PCSP. The CSPP must specify the type of events that require monitoring, the systems that will be subject to monitoring, how the monitoring will be handled, and the composition of the incident response team. The contractor must also provide security incident information to the DOE Office of Counterintelligence as necessary.

d. Cyber Security Advisories, Alerts, and Suspected Incidents. The contractor must respond to CIAC cyber security advisories, bulletins, alerts, and suspected incidents in accordance with the policy and procedures stated in the CSPP. The specific response must be commensurate with the level of risk and may include containment, remediation, and increased monitoring.

DEFINITIONS

Certification and Accreditation—Certification is the comprehensive evaluation of the technical and nontechnical security features of an Information System (IS) 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. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Critical Infrastructure Protection (CIP) Asset—A DOE asset that has been classified as critical by project Matrix or deemed critical by the Department element. A CIP asset must have a dedicated security plan.

Cyber Assets—All data, information, and components that create, store, display, transfer, and process electronic information (stand-alone and network).

Cyber Information—Data that supports one or more specific tasks or functions and is created, entered, processed, stored, displayed, or transmitted on or with an electronic system.

Cyber Security—Protection of information technology (IT) investments (e.g. information systems and telecommunications systems) and the information within or passing through them from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

- integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- availability, which means ensuring timely and reliable access to and use of information and information systems.

Cyber Security Competencies—The capabilities needed by individuals who create, possess, manage, operate, control, administer, document, or use DOE cyber assets. Competency is the necessary outcome, while training, education and awareness programs are common means to acquire the required competencies.

Cyber Security Management Program (CSMP)—Describes the program direction documentation to be issued to DOE organizations to establish how to comply with DOE O 205.1, *Departmental Cyber Security Management Program*, through the development of a PCSP and supporting CSPPs.

Cyber Security Program Plans (CSPPs)—Part of the program Secretarial office cyber security program. The plans provide specific information on planning, budgeting, implementing, operating, and maintaining cyber resources to fulfill program Secretarial office cyber security plans and the DOE Cyber Security Management Program.

Cyber Systems—See Information System.

DOE Elements—A term used for those DOE programs and administrations listed in Attachment 1.

General Support System—An interconnected set of information resources/information systems under the same direct management control which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN), including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center, including its operating system and utilities, or a shared information processing service organization.

Independent Verification and Validation (IV&V) Program—Independent reviews and assessments of the policies, processes, and procedures used by the DOE elements operating and protecting their cyber assets. IV&V results in recommendations for improvement of these policies, processes, and procedures.

Information System—Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes—

- computers and computer networks;
- ancillary equipment;
- software, firmware, and related procedures;
- services, including support services; and
- related resources.

Program Secretarial Office (PSO)—Departmental element with responsibility for specific programs or facilities.

Program Cyber Security Plan (PCSP)—Outlines how a DOE program Secretarial office or administration plans to implement and maintain cyber security for cyber assets/resources under its purview.

Remote Access—Entry into a DOE information system from outside of a DOE-controlled access point, using privileges granted to the user by the owning organization, through a process in which the user must identify and authenticate himself/herself to the system before session initiation.

SITE/FACILITY CONTRACTORS TO WHICH CRD APPLIES

Facility	Contractor
Management and Operating – *Research*	
Lawrence Berkeley National Laboratory	University Of California
Pacific Northwest National Laboratory	Battelle Memorial Institute
Brookhaven National Laboratory	Brookhaven Science Associates
Sandia National Laboratories	Lockheed Martin - Sandia Corp.
National Renewable Energy Laboratory	Midwest Research Institute
Stanford Linear Accelerator Center	Stanford University
Bettis Atomic Power Laboratory	Bechtel Bettis Inc
Argonne National Laboratory	University Of Chicago
Idaho National Engineering & Environmental Laboratory	Bechtel B&W Idaho LLC
Thomas Jefferson Nat'l Accelerator Facility	Southeastern Universities Res. Assoc.
Ames National Laboratory	Iowa State University
Oak Ridge National Laboratory	University of Tennessee/Battelle
Knolls Atomic Power Laboratory	Lockheed Martin-KAPL, Inc
Lawrence Livermore National Laboratory	University Of California
Los Alamos National Laboratory	University Of California
Savannah River Site	Westinghouse Savannah River Company
Princeton Plasma Physics Laboratory	Princeton University
Fermi National Accelarator Center	Universities Research Association
Management and Operating - *Plant/Facility*	
West Valley Project	Westinghouse-West Valley Nuc. Services
Strategic Petroleum Reserve	Dyn McDermott Petroleum Ops. Co.
Oak Ridge Y-12 Site	BWXT Y-12 LLC
Pantex Plant	BWXT Pantex LLC
Waste Isolation Pilot Plant	Westinghouse TRU Solutions
Nevada Test Site	Bechtel Nevada Corp
Kansas City Plant	Honeywell Federal Manufacturing & Tech.
National Civilian Radioactive Waste Program (Yucca Mtn)	Bechtel SAIC

Site Restoration	
Hanford Environmental Restoration	Bechtel Hanford Inc
Oak Ridge Environmental Management	Bechtel Jacobs Co LLC
Mound Environmental Management Project	BWXT of Ohio
Project Hanford	Fluor Daniel Hanford, Inc
River Protection Project Tank Farm Management	CH2M Hill Hanford Group
Rocky Flats	Kaiser Hill Co. LLC
Fernald Environmental Management Project	Fluor Daniel Env. Rest. Mgmt. Co.

Other	
Grand Junction Technical & Remediation Services	MACTEC Inc.
Grand Junction Facilities & Operations Services	Wastren Inc.
Oak Ridge Institute of Science & Education	Oak Ridge Associated Universities
Occupational Health Services at the Hanford Site	Hanford Environmental Health Foundation