

**SUBJECT: DEPARTMENT OF ENERGY CYBER SECURITY MANAGEMENT**

---

1. **PURPOSE.** The Department of Energy's (DOE's) overarching mission to advance the national, economic, and energy security of the United States and promote scientific and technological innovation is enabled, advanced, and reliant on information and information systems, which must be protected to ensure mission success. This directive establishes the high-level Departmental Cyber Security Management (CSM) structure for ensuring the protection of information and information systems<sup>1</sup>.
  
2. **OBJECTIVES.** CSM objectives are to—
  - a. establish line management accountability through Senior DOE Management [Under Secretaries, NNSA Administrator, Energy Information Administration, Power Marketing Administrations, and Chief Information Officer (CIO)] for ensuring protection of information and information systems.
  
  - b. provide Senior DOE Management with a framework and technical and management requirements for applying cyber security controls to meet mission-specific objectives.
  
  - c. protect information and information systems in accordance with statutory requirements, regulations, Presidential and Office of Management and Budget (OMB) directives, applicable Federal standards and guidance, and Departmental cyber security policy and technical and management requirements.
  
  - d. establish a program based on a federated approach that integrates cyber security governance, accountability, and reporting into management and work practices at all levels in the Department according to DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.
  
  - e. ensure that cyber security management processes are integrated with DOE strategic and operational planning processes.
  
  - f. establish a cost-effective risk management approach to protecting information and information systems.
  
  - g. establish high-level requirements and responsibilities for protecting unclassified and national security information and associated information systems.
  
  - h. establish a Departmental CSM structure that can adapt to emerging technologies and respond to the evolving threat environment.

---

<sup>1</sup> Unless explicitly noted, herein after, this includes all unclassified and national security systems.

- i. establish a training, education, and awareness program that develops and maintains cyber security competencies throughout DOE Federal and contractor workforces and enables personnel to fulfill their responsibilities in protecting DOE information and information systems.
  - j. provide for continuous improvement of the DOE cyber security program and posture.
3. CANCELLATIONS. DOE O 205.1, *Department of Energy Cyber Security Management Program*, dated 3-21-03. Cancellation of a directive does not by itself modify or otherwise affect any contractual obligation to comply with directive requirements. Canceled 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 canceled directives.

4. APPLICABILITY.

- a. Departmental Elements. Except for the exclusions in paragraph 4c, this Order applies to Departmental elements. (Go to <http://www.directives.doe.gov/pdfs/reftools/org-list.pdf> for the most current listing of Departmental elements. This list automatically includes Departmental elements created after the Order is issued.)

The Administrator of the National Nuclear Security Administration (NNSA) will assure that NNSA employees and contractors comply with their respective responsibilities under this directive. Nothing in this Order shall be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

- b. DOE Contractors.
  - (1) Except for the exclusions in paragraph 4c, the contractor requirements document (CRD), Attachment 1, sets forth requirements of this Order that will apply to contracts that include the CRD.
  - (2) The CRD must be included in contracts that include access to information and information systems used or operated by a contractor or other organization on behalf of DOE, including NNSA.
  - (3) The Head of the Departmental element is responsible for notifying the contracting officer of which contracts are affected. Once notified, the contracting officer is responsible for incorporating the CRD and applicable Program Cyber Security Plan (PCSP) into each affected contract.

- c. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, section 7, 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 will implement and oversee all requirements and practices pertaining to this DOE Order for activities under the Deputy Administrator's cognizance.

5. REQUIREMENTS.

a. CSM Direction.

- (1) Senior DOE Management has direct responsibility and accountability for—
  - (a) issuing direction for implementing cyber security within their respective organizations;
  - (b) determining, assessing, and documenting program-unique threats and risks (in addition to those presented in the Departmental Cyber Security Threat Statement and Risk Assessment); and
  - (c) developing PCSPs for the implementation of cyber security requirements in all organizations under their purview.
- (2) At a minimum, Power Marketing Administration (PMA) protections must also be in accordance with North American Electric Reliability Council (NERC) standards.

b. Program Cyber Security Plans.

- (1) Development of PCSPs. PCSPs must be developed for the following organizations in accordance with this Order:
  - NNSA<sup>2</sup>;
  - The Office of Energy<sup>2</sup>;
  - The Office of Science<sup>2</sup>;
  - The PMAs (a single PCSP template applicable to all PMAs is required); and

---

<sup>2</sup> Information systems operated by the CIO within DOE Headquarters must comply with the DOE CIO PCSP. Mission-specific information systems operate under a Senior DOE Management PCSP, unless the senior manager elects to utilize the DOE CIO PCSP. The Senior DOE Management PCSP used for systems operated at Headquarters must be consistent with the security controls governing boundary conditions of the Headquarters network as defined in the DOE CIO PCSP prior to connection to the network infrastructure.

- The Office of the Chief Information Officer (OCIO). The DOE CIO PCSP applies to all DOE staff offices.
- (2) Use of DOE CIO PCSPs. Heads of Departmental elements, including the Energy Information Administration (EIA), with subordinate elements outside DOE Headquarters facilities and who are not required by this Order to prepare a PCSP may use the DOE CIO PCSP or an extension of the DOE CIO PCSP, or develop a PCSP unique to the element for those subordinate elements outside DOE Headquarters.
  - (3) Unclassified Information Systems. PCSPs and other cyber security documentation must comply with the Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, OMB directives, Federal Information Processing Standards (FIPS), Departmental policies, and DOE CIO Cyber Security Technical and Management Requirements.
  - (4) National Security Systems. PCSPs and other cyber security documentation must comply with FISMA; Committee on National Security Systems (CNSS) policies and directives; Executive orders; DOE directives; the National Industrial Security Program Operating Manual (NISPOM), 02-28-06; and National Security Telecommunications and Information Systems Security Instruction No. 1000, *National Information Assurance Certification and Accreditation Process*, April 2000, and comply with DOE CIO Cyber Security Technical and Management Requirements as they apply to national security data and information systems within DOE, including NNSA. Systems designated as Intelligence Systems are subject to the requirements of the Director of National Intelligence.
- c. Governance—CSESC.
- (1) A Departmental Cyber Security Executive Steering Committee (CSESC) is established consisting of the NNSA Administrator; the Under Secretary for Energy; the Under Secretary for Science; the Administrator for EIA; the Director of Health, Safety, and Security (HSS); one PMA Administrator<sup>3</sup>; and the CIO.
  - (2) The CIO—
    - (a) serves as CSESC chairperson and
    - (b) oversees the DOE cyber security program.

---

<sup>3</sup> The PMA administrators will select initial representation among the PMA Administrators. The PMA administrators will determine rotation of the PMA representative on the CSESC.

- (c) with the advice of the CSESC and the support of the Departmental Cyber Security Working Group (CSWG), develops Departmental cyber security policy and DOE CIO Cyber Security Technical and Management Requirements consistent with FISMA, Presidential Directives and Executive Orders, OMB directives, FIPS, and policies promulgated by the CNSS.
  - (3) Each CSESC member must identify, in writing, an individual to serve on the CSWG.
  - (4) The CSWG serves as staff for the CSESC and supports actions and coordination of the DOE cyber security program.
- d. CSM and PCSP Implementation. Senior DOE Management is responsible for ensuring implementation of DOE cyber security program and the respective PCSPs under their purview. Requirements and responsibilities promulgated in the PCSP will flow down from Senior DOE Management to all subordinate organizational levels.
  - (1) Risk Management. Departmental elements must use a documented risk-based approach, in accordance with their applicable PCSP, to make informed decisions for protecting information and information systems under their purview, including the adequacy and maintenance of protection, cost implications of enhanced protection, and acceptance of risk.
  - (2) PCSP Development and Maintenance.
    - (a) PCSPs are living documents that must be developed, approved, and maintained to comply with FISMA, Presidential directives and Executive orders, OMB directives, FIPS, policies promulgated by the CNSS, Departmental policies, and DOE CIO Cyber Security Technical and Management Requirements.
    - (b) PCSPs must be reviewed, updated, and reapproved at least every 2 years.
  - (3) PCSP Use and Access. Senior DOE Management or their designees must maintain approved copies of PCSPs for auditing and monitoring purposes.
  - (4) Implementation Schedule. Within 90 days of issuance, Senior DOE Management must implement this Order and develop PCSPs.
- e. Compliance.
  - (1) All Departmental elements must comply with Department cyber security policies, DOE CIO Cyber Security Technical and Management Requirements, and the requirements specified in their respective PCSPs.

- (2) Conformance will be measured and reported to the DOE CIO through the respective Under Secretaries or NNSA Administrator based on Departmental policies and DOE CIO Cyber Security Technical and Management Requirements.

6. RESPONSIBILITIES.

a. Chief Information Officer.

- (1) Chairs the CSESC and appoints the chair of the CSWG.
- (2) Coordinates and provides the Department's response for all agency-level inquiries (e.g., Congressional and OMB), reporting, and program review requirements for cyber security.
- (3) Leads the development of and maintains Departmental cyber security Policies, Orders, Manuals, and bulletins.
- (4) Develops and issues DOE CIO Cyber Security Technical and Management Requirements, including those that augment or interpret FIPS and NIST cyber security SP 800-series publications.
- (5) Provides advice and assistance to Senior DOE Management and field organizations in all aspects of cyber security.
- (6) Retain overall management responsibility and accountability for information and information systems used or operated by DOE, including NNSA, or by a contractor or other organization on behalf of DOE, including NNSA.
- (7) Ensures the development and implementation of the DOE CIO PCSP a Headquarters PCSP that incorporates program-specific requirements with Departmental cyber security policies and DOE CIO Technical and Management Requirements.
- (8) Monitors the effectiveness of DOE CIO PCSP implementation through site assistance visits, program reviews, IG and HSS audits, compliance reviews, self-assessments, management assessments, analysis of performance measurement criteria, peer reviews, and vulnerability analyses.
- (9) Serves as the designated approving authority (DAA) for information systems covered by the DOE CIO PCSP.

NOTE: This authority may be further delegated to Senior Federal officials within the Departmental elements under CIO purview (but may not be delegated further). Although the authority for accepting risk may be delegated, the responsibility and accountability for ensuring that

information and information systems are protected and risk is being appropriately managed remains with the Chief Information Officer.

- (10) Ensures the official appointment of cyber security points of contact (documented in writing) for all Headquarters organizations and staff office organizations that will be responsible for ensuring the implementation of the PCSP in their organizations, and all subordinate organizations as appropriate.
- (11) Develops performance measurement processes and reports on CSM program performance to Senior DOE Management and other Government agencies, including OMB and the Congress.
- (12) Serves as the Department's primary point of contact for cyber security issues with other Federal agencies.
- (13) Establishes policy and guidance 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.
- (14) Oversees and manages the DOE CSM program through a federated approach whereby the OCIO is responsible for developing overall DOE cyber security strategy, and DOE CIO Cyber Security Technical and Management Requirements.
- (15) Develops, deploys, and manages the DOE OCIO Compliance Review Program. Coordinates review activity with Senior DOE Management, HSS, the Office of Intelligence and Counterintelligence, the Office of Inspector General, and relevant Departmental organizations, as required, to eliminate redundant reviews and provide opportunities to participate.
- (16) Develops and updates a baseline DOE cyber security threat statement and risk assessment in consultation with the Office of Intelligence and Counterintelligence, as needed or, at minimum, annually.
- (17) Coordinates the sharing of threat information with senior DOE management, the Office of Intelligence and Counterintelligence, and other U.S. Government officials.
- (18) Monitors plans for expenditure of DOE cyber security resources by supporting the Department's information technology capital planning processes for enterprise initiatives and procurements.

- (19) Determines, authorizes, declares, and communicates Information Conditions (INFOCONs) for the Department, including NNSA, to establish and maintain a defensive posture against the intentional disruption of information systems and networks.
- (20) Manages Department-wide cyber security incident reporting, assessment, and response activities in coordination with the Office of Inspector General (IG), other Departmental elements, and other U.S. Government organizations as circumstances warrant.
- (21) Coordinates the assessment of cyber security incidents. When a violation of law is suspected or the incident may be of counterintelligence interest, an investigation is initiated by appropriate authorities, the Inspector General or the Office of Intelligence and Counterintelligence. In such cases, OCIO response and assessment activities are carried out in cooperation with the investigation.
- (22) Reviews findings of IG and Government Accountability Office (GAO) cyber security audits and evaluations and ensures appropriate action in response to audit findings.
- (23) Reviews findings of HSS assessments and evaluations and ensures appropriate action in response to these findings.
- (24) Develops and maintains a process and guidance for documenting and monitoring the correction of significant cyber security deficiencies and systemic weaknesses in DOE.
- (25) Establishes and manages the DOE cyber security training, education, and awareness program.

b. DOE Under Secretaries and NNSA Administrator.

- (1) Retain overall management responsibility and accountability for information and information systems used or operated by DOE, including NNSA, or by a contractor or other organization on behalf of DOE, including NNSA.
- (2) Accept the overall cyber security risk for their organizations and field sites.
- (3) Serve as the DAA for all information systems covered by their PCSPs.

NOTE: This authority may be delegated to Senior Federal officials within the Departmental elements under their purview (but may not be delegated further). Although the authority for accepting risk may be delegated, the responsibility and accountability for ensuring that information and



information systems are protected and risk is being appropriately managed remains with the Under Secretary or Administrator.

- (4) Establish, assess, and implement INFOCON defensive posture(s) for their organization based on evaluation of all relevant factors. All Elements within the organization must remain at least as high as the current INFOCON directed by the DOE CIO.
- (5) Serve on the CSESC.
- (6) Identify and document in writing organization representatives on the CSWG.
- (7) Ensure that contract award fee determinations include an evaluation of cyber security effectiveness with a weight or importance at least commensurate with that of physical security or safety in each contract.
- (8) Identify and implement appropriate cyber security related incentives and disincentives for those sites and contractors without award fees.
- (9) Ensure the development and implementation of a PCSP that incorporates program specific requirements and the requirements of Departmental cyber security policies and DOE CIO Cyber Security Technical and Management Requirements.
- (10) Appoint and document in writing a Q-cleared cyber security point of contact responsible for ensuring the implementation of the PCSP throughout the organization.
- (11) Ensure that cyber security points of contact are appointed and documented in writing for all subordinate organizations that are responsible for implementing the organization PCSP.
- (12) Ensure that sufficient resources are identified, planned, budgeted, and deployed to implement and maintain the PCSP and maintain an effective risk management-based cyber security posture throughout the organization.
- (13) Monitor PCSP implementation effectiveness through site assistance visits, program reviews, IG and HSS audits, compliance reviews, self-assessments, management assessments, analyses or performance measurement criteria, peer reviews, and vulnerability analyses.
- (14) Ensure cyber security training, education, and awareness programs are implemented for management, system administrators, and all information system users in accordance with OCIO Training, Education and Awareness Program.

- (15) Support the OCIO in the development of Departmental cyber security policies and DOE CIO Cyber Security Technical and Management Requirements.
- (16) Notify contracting officers which contracts are affected by requirements of the CRD.

c. Cyber Security Executive Steering Committee Members.

- (1) Participate on the CSESC as outlined in the ESC charter.
- (2) Coordinate Departmental cyber security efforts to ensure efficient use of Departmental resources.
- (3) Provide direction to their constituent organizations and to supporting contractors.

d. Heads of Departmental Elements (other than Under Secretaries and NNSA Administrator).

- (1) Retain overall management responsibility and accountability of information and information systems used or operated by DOE, including NNSA, or by a contractor or other organization on behalf of DOE, including NNSA.
- (2) Accept overall cyber security risk for their organizations and field sites.
- (3) Serve as the DAA for all information systems under their control.

NOTE: This authority may be delegated to Senior Federal officials within the Departmental elements under their purview (but may not be delegated further). Although the authority for accepting risk may be delegated, the accountability and responsibility for ensuring that information and information systems are protected and risk is appropriately managed remains with the Head of the Departmental Element.

- (4) Ensure the development and implementation of a PCSP, adopt the DOE CIO PCSP, or incorporate program-specific requirements and guidance for all subordinate organizations into an extension of the DOE OCIO PCSP.
- (5) Ensure that contract award fee determinations include an evaluation of cyber security effectiveness with a weight or importance at least commensurate with that of physical security or safety in each contract.
- (6) Identify and implement appropriate cyber security incentives and disincentives for those sites and contractors without award fees.

- (7) Appoint cyber security points of contact that will be responsible for ensuring implementation of the PCSP in the organization and all subordinate organizations.
  - (8) Ensure that sufficient resources are identified, planned, budgeted, and deployed to implement and maintain the PCSP and maintain an effective risk management based cyber security posture throughout the organization.
  - (9) Monitor the effectiveness of program-specific PCSP implementation through site assistance visits, program reviews, IG and HSS audits, compliance reviews, self-assessments, management assessments, analysis of performance measurement criteria, peer reviews, and vulnerability analyses.
  - (10) Review audit findings and recommend response actions for improving the CSM.
  - (11) Notify contracting officers of which contracts are affected by requirements of the CRD.
- e. Chief Financial Officer. Coordinates cyber security budgets and funding with the CSESC and OCIO, as appropriate.
- f. Office of Health, Safety, and Security.
- (1) Coordinates an independent oversight program for evaluating CSM implementation.
  - (2) Conducts information system penetration testing as part of announced and unannounced cyber security inspections.
  - (3) Provides feedback to the OCIO and Senior DOE Management organizations on the effectiveness of DOE cyber security policy implementation and recommends improvements for cyber security programs.
  - (4) Conducts the annual evaluation of cyber security on national security information systems.
  - (5) Coordinates with the Office of Intelligence and Counterintelligence for the annual review of national security information systems processing intelligence information.
  - (6) Provides input to the Office of Inspector General for the annual evaluation of unclassified cyber security programs.

- (7) Solicits recommendations for cyber security inspection activities and focus areas from the CIO, IG, and Office of Intelligence and Counterintelligence.
- (8) Notifies Senior DOE Management, Office of the Inspector General, Office of Intelligence and Counterintelligence and heads of Departmental elements of scheduled inspections and provides opportunities to participate.

g. Office of Intelligence and Counterintelligence.

- (1) Manages cyber programs designed to detect, deter, investigate, exploit, and neutralize technical intelligence activities, espionage, sabotage, and international terrorist activities directed against DOE cyber assets.
- (2) Through the Cyber Directorate, provides cyber services to DOE in accordance with Office of Intelligence and Counterintelligence directives.
- (3) Serves as the DAA for national security information systems that process intelligence information. When an intelligence system includes DOE Restricted Data information assets, the system will be accredited by the DAA for intelligence systems using the governing intelligence community directives. Certification and accreditation results will be provided to appropriate Departmental elements for review.
- (4) Interprets and implements Director of National Intelligence directives governing the processing of intelligence information.
- (5) Coordinates investigations and disseminates threat information and relevant technical information from the U.S. Intelligence community resources.
- (6) Acts as the primary liaison with the Intelligence community on intelligence and technical vulnerability issues, FISMA, certifications and accreditations of national security intelligence systems.
- (7) Provides relevant threat information to Senior DOE Management to assist in the development, improvement, and maintenance of the CSM program and PCSPs.
- (8) Coordinates investigations, as appropriate, with the Office of Inspector General. Reports all suspected or alleged criminal cyber matters to the Office of Inspector General.

h. Office of Inspector General.

- (1) Coordinates cyber security audits and investigations with Senior DOE Management, HSS, the Office of Intelligence and Counterintelligence, and

other Departmental elements unless the IG determines that coordination might jeopardize the progress or completion of an IG audit, inspection, or investigation.

- (2) Conducts the annual evaluation of cyber security of all unclassified information systems.
  - (3) Conducts investigations of intrusions and anomalous activity on DOE information systems, when appropriate.
  - (4) Coordinates investigative activity concerning cyber security with Senior DOE Management, HSS, the Office of Intelligence and Counterintelligence, relevant Departmental organizations, and law enforcement agencies as required.
  - (5) Provides relevant criminal threat information to Senior DOE Management to assist in CSM development, improvement, and maintenance.
  - (6) Provides feedback to the OCIO on the effectiveness of DOE cyber security policy and DOE CIO Cyber Security Technical and Management Requirements implementation and recommends improvements for cyber security programs.
- i. Contracting Officers, once notified of contractor applicability, incorporate the CRD into affected contracts.
7. REFERENCES. See Appendix A.
  8. NECESSITY FINDINGS STATEMENT. “In compliance with Sec. 3174 of Pub. L. 104-201 (42 USC 7274 note), DOE hereby finds that this Order is necessary for the protection of human health and the environment or safety, fulfillment of current legal requirements, and conduct of critical administrative functions.”
  9. CONTACT. Questions concerning this Order should be directed to the OCIO at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:



CLAY SELL  
Deputy Secretary

## REFERENCES

1. Public Laws (P.L.).
  - a. P.L. 101-576, Chief Financial Officers (CFOs) Act of 1990, which lays a foundation for comprehensive reform of federal financial management and establishes a leadership structure, provides for long-range planning, requires audited financial statements, and strengthens accountability reporting.
  - b. P.L. 103-356, Government Management Reform Act of 1994, which requires improving the efficiency of executive branch performance such as the elimination or consolidation of duplicative or obsolete reporting requirements and adjustments to deadlines to provide for more efficient workload distribution or improve the quality of reports.
  - c. P.L. 104-13, Paperwork Reduction Act of 1995 (PRA), which requires that Federal agencies become more responsible and publicly accountable for reducing the burden of Federal paperwork on the public.
  - d. P.L. 104-208, Title VIII, Federal Financial Management Improvement Act of 1996 (FFMIA), which requires consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal government in order to increase the accountability and credibility of federal financial management.
  - e. P.L. 104-23, Electronic Freedom of Information Act (e-FOIA, enacted October 1996)--(Title 5 U.S.C. section 552), which requires agencies of the Federal government to make certain information available for public inspection and copying and to establish and enable enforcement of the right of any person to obtain access to the records except for those protected by statutory exemptions.
  - f. P.L. 105-277, Title XVII, Government Paperwork Elimination Act (GPEA, enacted October 1998), which requires that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives.
  - g. P.L. 107-347, Title III, Federal Information Security Management Act of 2002 (FISMA, enacted December 2002), which defines a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
  - h. P.L. 93-579, Privacy Act of 1974, as amended [Title 5 United States Code (U.S.C.) Section 552a], which prohibits disclosure of information in personal records by any means of communication to any person, or to another Agency except pursuant to a written request by or with the prior written consent of the individual to whom the records pertain.

- i. P.L. 96-349, Trade Secrets Act (18 U.S.C., section 1905), as amended, which defines the unlawful disclosure of confidential information and the penalties thereof.
  - j. P.L. 97-255, Federal Managers' Financial Integrity Act of 1982 (FMFIA), which defines requirements for Executive agency accounting and financial management reports and plans and identification and reporting of material weaknesses [Section 2, (d)(4)].
  - k. P.L. 99-474, Computer Fraud and Abuse Act of 1992- (18 U.S.C. section 1030), which defines the specific actions considered to be computer fraud or abuse.
  - l. P.L. 99-508, Electronic Communications Privacy Act of 1986, which amends 18 U.S.C. Chapter 119 with respect to intercepting certain communications and other forms of surveillance and for other purposes and prohibits unauthorized access to electronic communications systems to obtain or alter information and prohibits the installation or use of a pen register or tracking device without a court order.
  - m. P.L.103-62, Government Performance and Results Act of 1993 (GPRA), which provides for establishment of strategic planning and performance measurement in the Federal government.
  - n. P.L.104-106, Division E, Clinger-Cohen Act (Information Technology Management Reform Act of 1996), which defines reforms in information technology acquisition management within the Federal government.
2. Office of Management and Budget (OMB) Circulars.
- a. A-11, Planning, Budgeting, Acquisition of Capital Assets, Strategic Plans, Performance Plans, which provides guidance on budget submissions; instructions on budget execution, integrating Agencies' budget and accounting functions, and improving the quality of financial information in accordance with the Government Performance and Results Act of 1993 and other laws; and specific steps that agencies must take to integrate budget and performance, a key part of the President's Management Agenda.
  - b. A-76, Performance of Commercial Activities (Outsourcing), which establishes Federal policy for commercial activities and sets forth the procedures for determining whether commercial activities should be performed under contract with commercial sources or in-house using Government facilities and personnel.
  - c. A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs, which is general guidance for conducting benefit-cost and cost-effectiveness analyses and specific guidance on the discount rates to be used in evaluating Federal programs whose benefits and costs are distributed over time.

- d. A-123, Management Accountability and Control, which is guidance on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls in accordance with the Federal Managers' Financial Integrity Act of 1982 (FMFIA).
  - e. A-127, Financial Management Systems, which prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems in accordance with the Federal Managers' Financial Integrity Act of 1982 (FMFIA) and the Chief Financial Officers (CFOs) Act of 1990.
  - f. A-130, Management of Federal Information Resources, which establishes policy for the management of Federal information resources in accordance with the Computer Security Act of 1987.
  - g. A-130, Appendix III, Security of Federal Automated Information Resources, which establishes a minimum set of controls to be included in Federal automated information security programs, assigns Federal agency responsibilities for the security of automated information and incorporates requirements of the Computer Security Act of 1987 and responsibilities assigned in applicable national security directives.
3. OMB Memoranda Pertaining to IT Security and Management.
- a. M-95-22, Implementing the Information Dissemination Provisions of the Paperwork Reduction Act of 1995 (September 29, 1995).
  - b. M-96-20, Implementation of the Information Technology Management Reform Act of 1996 (April 4, 1996).
  - c. M-97-02, Funding Information Systems Investments (October 25, 1996).
  - d. M-97-16, Information Technology Architectures (June 18, 1997).
  - e. M-98-04, Annual Performance Plans Required by the Government Performance and Results Act (GPRA) (January 29, 1998).
  - f. M-99-05, Instructions for Complying With The President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records, (January 7, 1990).
  - g. M-99-18, Privacy Policies on Federal Web Sites (June 2, 1999).
  - h. M-99-20, Security of Federal Automated Information Resources (June 23, 1999).
  - i. M-00-07, Incorporating and Funding Security in Information Systems Investments (February 28, 2000).



- j. M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act (April 25, 2000).
  - k. M-00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000).
  - l. M-00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act (September 25, 2000).
  - m. M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy (December 20, 2000).
  - n. M-01-08, Guidance On Implementing the Government Information Security Reform Act (January 16, 2001).
  - o. M-01-26, Component-Level Audits (July 10, 2001).
  - p. M-02-12, Reducing Redundant IT Infrastructure to Homeland Security (July 19, 2002).
  - q. M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 30, 2003).
  - r. M-04-04, E-Authentication Guidance (December 16, 2003).
  - s. M-04-16, Software Acquisition (July 1, 2004).
  - t. M-04-26, Personal Use Policies and “File Sharing” Technology (September 8, 2004).
  - u. M-05-02, Financial Management Systems (December 1, 2004).
  - v. M-05-04, Policies for Federal Agency Public Websites (December 17, 2004).
  - w. M-05-05, Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services (December 20, 2004).
  - x. M-05-08, Designation of Senior Agency Officials for Privacy (February 11, 2005).
  - y. M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 17, 2006).
4. DOE Orders, Manuals, Notices, and Guidelines.
- a. DOE O 142.3, *Unclassified Foreign Visits and Assignments*, dated 6-18-04.
  - b. DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.

- c. DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 3-22-01.
  - d. DOE O 221.2, *Cooperation with the Office of Inspector General*, dated 3-22-01.
  - e. DOE P 226.1, *Department of Energy Oversight Policy*, dated 6-10-05.
  - f. DOE O 226.1, *Implementation of Department of Energy Oversight Policy*, dated 9-15-05.
  - g. DOE N 221.12, *Reporting Fraud, Waste, and Abuse*, dated 10-19-06.
  - h. DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, dated 5-8-01.
  - i. DOE O 470.2B, *Independent Oversight and Performance Assurance Program*, dated 10-31-02.
  - j. DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00.
  - k. DOE O 470.4, *Safeguards and Security Program*, dated 8-26-05.
  - l. DOE O 475.1, *Counterintelligence Program*, dated 12-10-04.
5. Other.
- a. Executive Order (E.O.) 13231 - Critical Infrastructure Protection in the Information Age (October 16, 2001) - The purpose of this Order is to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible.
  - b. E.O. 13228 - Establishing the Office of Homeland Security and the Homeland Security Council (October 8, 2001) - This Executive Order establishes within the Executive Office of the President an Office of Homeland Security (the "Office") to be headed by the Assistant to the President for Homeland Security.
  - c. Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003) superseded The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (May 22, 1998) to ensure the viability of national infrastructures that are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

- d. Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004).
- e. National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems. This directive establishes initial objectives of policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation.
- f. Issuances of the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC), [Policies (P), Directives (D), and Instructions (I)].
  - (1) National Security Telecommunications and Information System Security Policy No. 11, *National Information Assurance Acquisition Policy*, dated July 2003.
  - (2) National Security Telecommunications and Information Systems Security Committee Directive No. 500, *Information Systems Security (INFOSEC) Education, Training, and Awareness*, dated 25 February 1993.
  - (3) National Security Telecommunications and Information Systems Security Committee Directive No. 501, *National Training Program for Information Systems Security (INFOSEC) Professionals*, dated 16 November 1992.
  - (4) National Security Telecommunications and Information Systems Security Advisory Memorandum INFOSEC 1-99, *The Insider Threat to U. S. Government Information Systems*, dated July 1999.
  - (5) National Security Telecommunications and Information System Security Instruction No. 1000, *National Information Assurance Certification and Accreditation Process*, dated April 2000.
- g. National Industrial Security Program Operations Manual, dated February 2006.
- h. Atomic Energy Act of 1954 as amended.
- i. E.O. 13011, "Federal Information Technology," dated 7-17-96.
- j. E.O. 12344, "Naval Nuclear Propulsion Program," dated 2-1-82.
- k. E.O. 12958 "Classified National Security Information," dated 4-17-95.
- l. NIST FIPS-199, Standards for Security Categorization of Federal Information and Information Systems.

- m. NIST FIPS-200, Minimum Security Requirements for Federal Information and Information Systems.
- n. NIST Special Publications 800 series.

**CONTRACTOR REQUIREMENTS DOCUMENT**  
**DOE O 205.1A, *Department of Energy Cyber Security Management Program***

Regardless of the performer of the work, the contractor is responsible for compliance with the provisions and requirements of this CRD and flowing down CRD requirements to subcontractors at any tier to ensure the contractor's compliance with these provisions and requirements. As directed by the contracting officer, the contractor must meet the following requirements.

The contractor must implement and comply with the applicable Program Cyber Security Plan (PCSP), as provided by Senior DOE Management, for all cyber security activities involving unclassified or national security information systems; compliance with the PCSP is monitored by Senior DOE Management.