Department of Energy

Oak Ridge Office
P.O. Box 2001
Oak Ridge, Tennessee 37831—

May 20, 2008

Mr. Brian W. Smith, Chief
Enrichment and Conversion Branch
Division of Fuel Cycle Safety and Safeguards
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
MS: EBB2-C40M
Washington, DC 20555-0001

Dear Mr. Smith:

REVISED DEPARTMENT OF ENERGY REQUIREMENTS FOR ACCREDITATION OF CLASSIFED CYBER SYSTEMS

Per our discussion, please find enclosed documents to implement new requirements relative to removable medium recently promulgated by the Department of Energy (DOE) for classified cyber systems. These documents are:

- DOE Order 205.1A --- Department of Energy Cyber Security Management
- DOE Manual 205.1-4 --- National Security System Manual

These documents provide requirements for DOE's accreditation of classified cyber systems and should be provided to your licensees which have classified cyber systems that will be accredited by DOE.

Please contact me at (865) 241-8277, if you should have any questions.

Sincerely,

George Herron

for Randall M. DeVault
Regulatory Oversight Manager
Office of Assistant Manager
for Nuclear Fuel Supply

Enclosure

cc's on page 2

PRINTED ON RECYCLED PAPER

cc w/o enclosure:
L. Clark, NS-50, ORO
M. Heiskell, NS-51, ORO
R. Holt, AD-41, ORO
D. Level, NS-52, ORO
Q. Nguyen, AD-41, ORO
S. Rice, OS-201, ORO
K. Walling, CC-10, ORO
K. Everly, NRC, White Flint

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

ORDER

DOE O 205.1A

Approved: 12-4-06

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[1].

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.

---

[1] 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[2];
- The Office of Energy[2];
- The Office of Science[2];
- The PMAs (a single PCSP template applicable to all PMAs is required) and

[2] 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[3]; and the CIO.

(2) The CIO—

(a) serves as CSESC chairperson and

(b) oversees the DOE cyber security program.

---

[3] 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 PSCP 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.

MANUAL

DOE M 205.1-4

Approved: 3-8-07

NATIONAL SECURITY SYSTEM MANUAL

U.S. DEPARTMENT OF ENERGY
Office of the Chief Information Officer

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of the Chief Information Officer

NATIONAL SECURITY SYSTEM MANUAL

1. PURPOSE. This Department of Energy (DOE) Manual provides requirements for the implementation of the following:

   a. Committee on National Security Systems Policy No. 6, National Policy on Certification and Accreditation of National Security Systems;

   b. National Security Telecommunications and Information System Security Instruction No. 1000, *National Information Assurance Certification and Accreditation Process*;

   c. National Industrial Security Program Operating Manual; and

   d. DOE cyber security program criteria for the implementation of management, operational, and technical controls for DOE, including National Nuclear Security Administration (NNSA), National Security Systems.

2. CANCELLATIONS. DOE M 471.2-2, *Classified Information Systems Security Manual*, dated 8-3-99. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive. Contractor requirement documents (CRDs) that have been incorporated into or attached to a contract remain in effect until the contract is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. All Departmental Elements. Except for the exclusions in paragraph 3c, this Manual applies to Departmental elements that utilize National Security Systems to collect, process, store, display, create, disseminate, or transmit information. (Go to www.directives.doe.gov/pdfs/reftools/org-list.pdf for the current listing of Departmental elements. This list automatically includes Departmental elements created after the Manual 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 Manual. Nothing in this Manual will 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 3c, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Manual that will apply to site/facility management contracts that include the CRD.

(2) This CRD must be included in all contracts that involve National Security Systems that are used or operated by a contractor or other organization on behalf of DOE, including NNSA, to collect, process, store, display, create, disseminate, or transmit information.

(3) The heads of Departmental Elements are responsible for notifying contracting officers of affected site/facility management contracts to incorporate this directive into those contracts. Once notified, contracting officers are responsible for incorporating the CRD into each affected contract via the *Laws, Regulations, and DOE Directives* clause of the contracts within 90 days.

(4) A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy act of 1954 (42 U.S.C. 228b.). The procedures for assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, (10 CFR 824).

(5) As stated in DEAR clause 970, 5204-2, titled *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this CRD and only incur costs that would be incurred by a prudent person in the conduct of competitive business.

(6) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Manual to other than site/facility management contracts will be communicated as follows:

(a) Heads of Field Elements and Headquarters Departmental Elements. Review procurement requests for new non-site/facility management contracts that involve National Security Systems and contain DEAR clause 952.204-2, *Security Requirements*. If appropriate, ensure that the requirements of the CRD of this Manual are included in the contract.

(b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of the CRD of this

Manual in new non-site/facility management contracts, as appropriate.

c. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, section 7, the Director, 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 Manual for activities under the Deputy Administrator's cognizance.

4. OBJECTIVES.

a. To ensure that Senior DOE Management Program Cyber Security Plans (PCSPs) are consistent with and achieve the objectives of Executive Orders, National Security Directives, Federal regulations, and national level policy.

b. To establish baseline requirements and assign responsibilities for protecting information on National Security Systems.

5. IMPLEMENTATION. This Manual is effective 30 days after issuance. However, DOE recognizes that this Manual cannot be implemented into Senior DOE Management PCSPs overnight. DOE expects that Senior DOE Management shall implement the criteria in this document within 90 days of its effective date. If Senior DOE Management cannot implement all of the criteria by the scheduled milestone, Senior DOE Management must establish a Plan of Actions and Milestones (POA&M) for implementation of this Manual in their PCSP.

a. Senior DOE Management must develop, and issue to each operating unit, mission oriented implementation policies for the criteria in this Manual. The Senior DOE Management PCSPs must require their operating units to implement and maintain at least the minimum requirements in this Manual for National Security Systems within 120 days of the release of the PCSP. If an operating unit cannot implement the requirements of this Manual, as documented in the PCSP, by the scheduled milestone, the operating unit must establish a POA&M for implementation of the PCSP requirements. Information systems designated as Intelligence Systems are subject to the requirements of the Director of National Intelligence and are therefore excluded from the requirements of this Manual.

b. Existing accredited national security systems shall remain accredited until reaccreditation is required, either because the systems have passed the 3-year accreditation expiration date or because of significant changes in the security requirements of the information system. After implementation of this Manual, reaccreditation must be in accordance with this Manual.

6. SUMMARY. This Manual is composed of two chapters that provide direction for the characterization of information, risk management, and security controls to be

implemented for National Security Systems and the responsibilities for managing cyber security. These chapters address mandatory procedures and management processes. Chapter I describes the requirements for the protection of National Security Systems based on the information groups. Chapter II describes the management responsibilities for implementing the requirements of Chapter I.

7. DEFINITIONS. This section contains only those terms unique to this specific Manual. Attachment 4 of DOE CIO Guidance CS-1, Management, Operations, and Technical Controls Guidance includes definitions of terms in all DOE CIO Guides and Manuals.

   a. **Authenticated User**. A user that has been properly identified and authenticated. These are considered legitimate users of the information system.

   b. **Certifier**. The Certification Agent and/ or the Designated Approving Authority responsible for conducting a comprehensive assessment of the technical, operational, and assurance controls in the information system.

   c. **System Owner**. The manager or other official responsible for the procurement, development, integration, modification, or operation and maintenance of the information system.

8. REFERENCES.

   a. Title XXXII of P.L. 106-65, National Nuclear Security Administration Act, as amended, which established a separately organized agency within the Department of Energy.

   b. Title 44, United States Code, Chapter 35, Subchapter III, § 3547. National security systems.

   c. E.O. 13010, *Critical Infrastructure Protection*, as amended, dated July 15, 1996.

   d. National Security Telecommunications and Information Systems Security Committee Directive No. 500, *Information Systems Security (INFOSEC) Education, Training, and Awareness*, dated 25 February 1993.

   e. National Security Telecommunications and Information Systems Security Committee Directive No. 501, *National Training Program for Information Systems Security (INFOSEC) Professionals*, dated 16 November 1992.

   f. National Security Telecommunications and Information Systems Security Advisory Memorandum INFOSEC 1-99, *The Insider Threat to U. S. Government Information Systems*, dated July 1999.

g. National Security Telecommunications and Information System Security Instruction No. 1000, *National Information Assurance Certification and Accreditation Process*, dated April 2000.

h. National Industrial Security Program Operating Manual, dated February 28, 2006.

9. CONTACT. Questions concerning this Manual should be addressed to the Office of the Chief Information Officer at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

CLAY SELL
Deputy Secretary

CONTENTS

1. PURPOSE. i
2. CANCELLATIONS. i
3. APPLICABILITY. i
4. OBJECTIVES. iii
5. IMPLEMENTATION. iii
6. SUMMARY iii
7. DEFINITIONS. iv
8. REFERENCES. iv
9. CONTACT v

CHAPTER I. REQUIREMENTS I-1

1. INTRODUCTION I-1
2. PROGRAM CYBER SECURITY PLANS I-1
3. INFORMATION CHARACTERIZATION I-2
4. RISK MANAGEMENT PROCESS I-7
5. SINGLE USER, STAND-ALONE INFORMATION SYSTEMS I-7
6. TECHNICAL CONTROLS I-7
7. OPERATIONAL CONTROLS I-31
8. ASSURANCE CONTROLS I-39

CHAPTER II. RESPONSIBILITIES II-1

ATTACHMENT 1 CONTRACTOR REQUIREMENTS DOCUMENT

CHAPTER I. REQUIREMENTS

1. INTRODUCTION. The DOE Under Secretaries (including the NNSA Administrator), the Energy Information Administration (EIA), the Power Marketing Administrations (PMAs), and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats not previously addressed or created in respect to the DOE and alignment between their subordinate organizations and contractors (hereafter called operating units), incorporating those requirements into their Program Cyber Security Plan (PCSP), and ensuring that those requirements are incorporated into contracts.

2. PROGRAM CYBER SECURITY PLANS.

   a. Senior DOE Management.

      PCSPs incorporating the requirements of this Manual must be developed as required by DOE O 205.1A, *Department of Energy Cyber Security Management Program*, dated 12-4-06, commensurate with the program-unique threats and risks (in addition to those presented in the Departmental Cyber Security Threat Statement and Risk Assessment).

   b. Use of DOE CIO PCSP.

      Heads of Departmental elements, including the Energy Information Administration (EIA), with subordinate elements outside DOE Headquarters facilities and who are not required by Order 205.1A 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.

   c. Supplemental Requirements.

      Organizations responsible for preparing PCSPs may specify and implement supplemental Senior DOE Management organizational requirements to address specific risks, vulnerabilities, or threats not previously addressed or created in respect to the DOE incorporating those requirements into their PCSP. PCSPs must include processes that allow operating units to specify and implement controls that address local or system specific risks, vulnerabilities, or threats not addressed by the PCSP.

   d. System Security Plans.

      (1) Each National Security System must be covered by a System Security Plan (SSP).

(2) The technical, operational, and assurance controls that comprise the minimum set of security controls for the system must be documented in the SSP, including any additional implementation information for the control. Any additional controls resulting from adjustments identified during the risk management process must also be included in the SSP.

(3) The SSP must address how the system implements the minimum technical, operational and assurance requirements identified in this Manual. If the Consequence of Loss (CoL) for confidentiality, integrity or availability has been increased by the Senior DOE Management or the operating unit or there is a threat not identified in the DOE Cyber Threat Statement, the SSP must describe the implementation of any additional controls.

(4) Common security controls defined in the PCSP or operating unit cyber security program can be technical (e.g., performed by a single system or device in a network), operational (e.g. the same purging procedure applies to all operating unit systems), or assurance (e.g. the same configuration management process used for multiple systems). Common security controls must be documented in at least one approved SSP associated with an accredited information system. The certification and accreditation of that system will verify that the control has been correctly implemented and is effective. Use of the control(s) in other information systems requires DAA-approved testing to validate correct implementation of the control(s) in the new information system. Other SSPs may reference that SSP for implementation documentation and certification test results.

3. INFORMATION CHARACTERIZATION.

National security information is grouped (information group) based on sensitivity (classification level, category, and need-to-know). The following paragraph describes the information groups used by the DOE in increasing order of sensitivity (Top Secret Restricted Data considered the most sensitive). National Security Systems must be categorized based on the most sensitive information group they contain and the impact/ CoL if the confidentiality, integrity and/or availability of the information is lost. The impact is determined through a CoL concept that ranks the perceived value of each information group in terms of confidentiality, integrity, and availability. A DOE evaluation has determined a minimum DOE CoL value for each information group.

a. Information Groups.

An information group contains all information types that require similar protection or are similar in content or use. The DOE CIO has identified a minimum set of national security information groups, not including SCI

information or information in special access programs. These information groups have been used in assessing the risk to information and in defining the minimum protection criteria for information systems containing each information group. The information groups and sub-groups are:

(1) Confidential/Secret (C/S)—Information that is classified as Confidential National Security Information, Confidential Formerly Restricted Data, Confidential Restricted Data, Secret National Security Information, or Secret Formerly Restricted Data and does not contain any nuclear weapons data.

(2) Secret Restricted Data (SRD)—Information that is classified Secret Restricted Data and does not contain any nuclear weapons data.

(3) Confidential Restricted Data, Sigmas 1 through 13 (CRD1-13)—Information that is classified as Confidential and identified as Restricted Data, Formerly Restricted Data, or is related to nuclear weapons contains information that falls in at least one of the sigma categories 1 through 13 as described in DOE O 5610.2, *Control of Weapon Data*, and successors.

(4) Secret Restricted Data, Sigmas 1 through 13, 15 and 20 (SRD1-13, 15, 20)—Information that is classified as Secret and identified as Restricted Data and is related to nuclear weapons and contains information that falls within at least one of the sigma categories 1 through 13, 15 and 20 as described in DOE O 5610.2, *Control of Weapon Data*, and successors.

(5) Secret Restricted Data, Sigma 14 (SRD14)—Information that is classified as Secret and identified as Restricted Data or is related to nuclear weapons and contains information that falls within the Sigma 14 category, as described in DOE O 5610.2, *Control of Weapon Data*, DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Design*, and DOE O 457.1, *Nuclear Counterterrorism*, respectively and their successors.

(6) Top Secret (TS)—Information that is classified as Top Secret National Security Information or Top Secret Formerly Restricted Data and does not contain any nuclear weapons data.

(7) Top Secret Restricted Data (TSRD)—Nuclear Weapons information that is classified Top Secret.

b. Consequence of Loss.

Table 1, Table 2, and Table 3 describe the criteria used to determine the CoL to confidentiality, integrity, and availability for all information groups. Table 4 provides the results of the DOE evaluation of impact of loss for each national

security information group and represents the minimum CoL value for confidentiality, integrity, and availability for each information group.

Table 1. Consequence of Loss of Confidentiality

Consequence of Loss	Confidentiality
Very High	Grave damage to National security will result if confidentiality is lost; or Information designated as life- or mission-critical.
High	Unauthorized, premature, or partial disclosure may have a serious effect on National security, Senior DOE Management, DOE, or National interests.
Medium	Serious damage to National security will result if confidentiality is lost; Information requiring protection mandated by policy, laws, or agreements between DOE, its contractors, and other entities, such as commercial organizations or foreign Governments; Information designated as mission-essential; or Unauthorized, premature, or partial disclosure may have an adverse effect on site-level interests.
Low	Damage to National security will result if confidentiality is lost; Information designated as sensitive by the data owner; or Unauthorized, premature, or partial disclosure may have an adverse effect on organizational interests.
Very Low	No damage to National security; and Information essentially requires no protection against disclosure.

Table 2. Consequence of Loss of Integrity

Consequence of Loss	Integrity
Very High	Grave damage to National security will result if integrity is lost or Information designated as life- or mission-critical.
High	Loss of integrity will have a serious effect on National-level interests or Loss of integrity will have a serious effect on confidentiality.
Medium	A degree of integrity required for mission accomplishment, but not absolute; Bodily injury might result from loss of integrity; or Loss of integrity will have an adverse effect on organizational-level interests.
Low	Loss of integrity impacts only the missions of site- or office-level organization.

Table 3. Consequence of Loss of Availability

Consequence of Loss	Availability
High	Loss of life might result from loss of availability; Information must always be available upon request, with no tolerance for delay; Loss of availability will have an adverse effect on National-level interests; Federal requirement (i.e., requirement for Material Control and Accountability (MC&A) inventory); or Loss of availability will have an adverse effect on confidentiality.
Medium	Information must be readily available with minimum tolerance for delay; Bodily injury might result from loss of availability; or Loss of availability will have an adverse effect on organizational-level interests.
Low	Information must be available with flexible tolerance for delay.
Very Low	Information availability is a low priority for system mission.

Note: In this context, "High – no tolerance for delay" means no delay; "Medium – minimum tolerance for delay" means a delay of seconds to hours; and "Low – flexible tolerance for delay" means a delay of days to weeks

Table 4. Consequence of Loss of Confidentiality, Integrity, and Availability

Protection Index	Information Group			Loss of Confidentiality	Loss of Integrity	Loss of Availability
PI-1	Confidential/Secret			Medium	Low	Very Low
PI-2	Secret Restricted			Medium	Low	Very Low
PI-3	Confidential Restricted Data	Sigma[1]	1, 2, 3, 4, 5, 9, 10, 11, 12, and 13	High	Low	Very Low
PI-4	Secret Restricted Data	Sigma	1, 2, 3, 4, 5, 9, 10, 11, 12, 13, 15, and 20	High	Low	Very Low
PI-5	Secret Restricted Data	Sigma	14	Very High	Low	Very Low
PI-6	Top Secret			Very High	Low	Very Low
PI-7	Top Secret Restricted Data			Very High	Low	Very Low

[1]Sigmas 6, 7, and 8 are not currently in use.

NOTE: The levels in this table are the minimum values allowed by DOE. Senior DOE Management or the operating unit may assign a higher level of consequence for any or all of the information groups.

4. RISK MANAGEMENT PROCESS.

The DOE Cyber Threat Statement identifies the threats to DOE information and information systems and the DOE Cyber Risk Assessment provides an assessment of the risks posed by the cyber threats. The DOE Cyber Threat Statement provides an assessment of the threats to DOE (including NNSA) information and information systems and the likelihood that a specified perpetrator will initiate threat activities. The DOE Cyber Risk Assessment evaluates the likelihood of threat activities against each information group and identifies the uncompensated risk to the information group and system on which it resides. The risk management process must be accomplished throughout the system lifecycle.

Each system must be categorized in order to identify the technical, operational, and assurance controls that comprise the minimum set of security controls for the system. Additional controls may be added (control adjustments) to implement supplemental requirements identified as a result of enterprise, operating unit, system, or data owner risk management reviews. The operating unit risk management process must include the following methods to characterize the system and implement and adjust the controls.

a. System Categorization.

The system categorization process consists of identifying the accreditation boundary of the information system (hardware, firmware, software, and connectivity), identifying each information group on information systems within the boundary of the system and determining the highest CoL for confidentiality for the system. The system can then be categorized using the information group with the highest confidentiality CoL. The Protection Index, see Table 4, is the index for selecting the technical, operational, and assurance controls that comprise the minimum security criteria for the system.

b. Controls Adjustment.

The Senior DOE Management PCSP must describe the process for adjusting the minimum controls described in this Manual. The controls are analyzed in light of any decision by Senior DOE Management, the operating unit, or information system owner to increase the CoL, identification of a threat not identified in the DOE Threat Statement, and/or identification of a standard practice not identified in the control set for a protection index. Additional controls above the minimum controls described for the protection index should be based on changes in the CoL, Threats, or standard practices.

5. SINGLE USER, STAND-ALONE INFORMATION SYSTEMS.

Extensive technical protection measures may be inappropriate and unnecessarily expensive for single-user, stand-alone information systems. Information systems that have one user at a time, but have more than one user with no sanitization between users, are multi-user information systems and are to fully comply with the requirements in this Manual implemented in the Senior DOE Management PCSP. Senior DOE Management PCSPs are to establish the process for determining which of the management, operational and technical controls contained in this Manual are to be applied to stand-alone, single-user information systems in the Senior DOE Management operating units.

6. TECHNICAL CONTROLS.

Technical controls rely on the information technology (IT) resource containing the information. Technical controls are intended to be implemented within the information system through means employing software, hardware, or firmware.

NOTES: The control identifier appears in the following tables to indicate that the control listed on the left must be implemented for the protection index across the top.

The parenthetical numbers following a control identifier in the table associate additional control enhancement(s) required for the protection indices; control enhancements identify applicable protection indices and are described with the corresponding control statement. The additional controls must be implemented in addition to the primary control.

Where bolded and italicized items are in the control statement, the PCSP or SSP developer must provide the information identified in the bracketed, ***italicized*** clause to describe the implementation.

a. Security Audit.

The PCSP must require each operating unit to implement the Security Audit controls listed in Table 5 pertaining to the indicated Protection Index for all national security systems under their responsibility. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them. These controls address the recognizing, recording, storing, and analyzing information related to security relevant activities.

Table 5. Security Audit Controls

Security Audit Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
AU-1	Security Alarms	AU-1	AU-1	AU-1	AU-1	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2	AU-2	AU-2	AU-2 (1)	AU-2 (1)	AU-2 (1)
AU-3	Audit Record Contents	AU-3	AU-3	AU-3	AU-3	AU-3 (1) (2)	AU-3 (1) (2)	AU-3 (1) (2)
AU-4	Profile Based Anomaly Detection	N/A	N/A	AU-4	AU-4	AU-4 (1)	AU-4 (1)	AU-4 (1)
AU-5	Complex Attack Heuristics	AU-5	AU-5	AU-5	AU-5	AU-5	AU-5	AU-5
AU-6	Audit Review	AU-6	AU-6	AU-6	AU-6	AU-6 (1)	AU-6 (1)	AU-6 (1)
AU-7	Guarantees of Audit Data Availability	AU-7	AU-7	AU-7	AU-7	AU-7 (1)	AU-7 (1)	AU-7 (1)

AU-1 SECURITY ALARMS

The information system security controls shall include or exclude auditable events from the set of audited events based on the user identity and role and shall automatically alert the Information System Security Officer (ISSO) and take [***list of actions (e.g., automatically lock out the system, isolate the system, no additional actions)***] upon detection of a potential security violation.

AU-2 AUDITABLE EVENTS

The information system shall provide the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail. The information system shall provide the capability to manage the selection of events to be audited by individual components of the system.

The information system security controls shall generate an audit record of the following events:

- Start-up and shutdown of the audit functions

- Successful use of the user security attribute administration functions
- All attempted uses of the user security attribute administration functions
- Identification of which user security attributes have been modified
- Successful and unsuccessful logons and logoffs
- Unsuccessful access to security relevant files including creating, opening, closing, modifying, and deleting those files
- Changes in user authenticators
- Blocking or blacklisting user Ids, terminals, or access ports
- Denial of access for excessive logon attempts
- System accesses by privileged users
- Privileged activities at the system console (either physical or logical consoles) and other system- level accesses by privileged users
- Starting and ending times for each access to the system

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall generate an audit record of the creation, deletion, or change of a security label. The information system shall be able to include or exclude auditable events from the set of audited events based on the subject sensitivity label; object sensitivity label; and source host identity.

AU-3 AUDIT RECORD CONTENTS

The audit record for each event shall contain at least the date and time of the event, type of event, user/role, object acted upon, and the outcome (success or failure) of the event.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall record within each audit record for each audit event the sensitivity labels of subject, object, or information involved; and source host identity.

Control Enhancement (2): For PI-5 through PI-7, the information system shall synchronize internal information system clocks at least daily.

AU-4 PROFILE BASED ANOMALY DETECTION

The information system security controls shall be able to maintain profiles of systems usage, where an individual profile represents the historical patterns of usage performed by single users and/or members of group accounts and/or [***profile target group(s) (e.g. users who share a group ID or group account, users who operate under an assigned role, users of an entire system or network node)***].

Control Enhancement (1): For PI-5 through PI-7, the information system shall employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. The information system shall employ automated mechanisms to alert security personnel of ***[list of additional inappropriate or unusual activities that are to result in alerts (e.g., Excessive login attempts across network; Access to privilege system files, Exceeding data quotas/transfers, Creation of account; Privileged account logged into multiple servers/ devices/applications; Attempts to access unauthorized sites/computers/devices/objects; Unauthorized shutdown/restart of system/device/application; Permission change for user/file/application; Use of privileged commands; and Unauthorized export from system to media)]***.

AU-5 COMPLEX ATTACK HEURISTICS

The information system security controls shall maintain an internal representation of the event sequences of known intrusion scenarios and signature events that may indicate a potential violation of information system security; compare the signature events and event sequences against a record of system activity; and alert security personnel and [***list of third parties (e.g., system owner, Alternate ISSO, network administrator)***] of a potential imminent violation of information system security when system activity is found to match a signature event or event sequence that indicates a potential violation of information system security.

AU-6 AUDIT REVIEW

The information system security controls shall provide the ISSO and authorized system administrators with the audit records and the capability to read all audit information from the audit records in a manner suitable for interpreting the information. Read access to the audit records shall be prohibited to all other users. The information system security controls shall provide the ability to perform searches, sorting, and ordering of audit

data based on user identity. Audit records shall be reviewed at least weekly and retained for at least one year.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall provide the ability to perform searches, sorting, and ordering of audit data based on subject sensitivity label, object sensitivity label, and source host identity.

AU-7 GUARANTEES OF AUDIT DATA AVAILABILITY

The stored audit records shall be protected from unauthorized deletion, prevent modification, and ensure that records already written (i.e. to media) will be maintained when the audit storage is exhausted, the system fails, or an attack occurs. An alarm (e.g. any clear indication that the pre-defined limit has been exceeded) shall be generated and provided to the ISSO and the authorized system administrator if the audit trail storage exceeds 80% of capacity. The information system shall prevent auditable events from being lost (e.g., deleted, overwritten, not recorded), except those taken by the ISSO or authorized system administrator if the audit trail has reached storage capacity.

Control Enhancement (1): For PI-5 through PI-7, the information system shall cease operations if the audit trail has reached storage capacity. The ISSO is the only person authorized to restart operations once sufficient audit capacity is available.

b. Communication.

The PCSP must require each operating unit to implement the Communication controls listed in Table 6 pertaining to the indicated protection index for all national security systems under their responsibility. These controls address assuring the identity of the originator and recipient of transmitted information.

Table 6. Communication Controls

Communication Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
CO-1	Proof of Origin	N/A	N/A	N/A	N/A	CO-1	CO-1	CO-1
CO-2	Proof of Receipt	N/A	N/A	N/A	N/A	CO-2	CO-2	CO-2

CO-1 PROOF OF ORIGIN

The information system security controls shall be able to generate evidence of origin for transmitted [***list of information types (e.g., Confidential/Secret, Secret RD, Confidential RD, Secret RD 1-13, etc).***at the request of the originator, recipient, ISSO, or [***list of third parties (e.g., system owner, ISSM, project management, etc.)***] and provide a capability to verify the evidence of origin of information to the originator, recipient, or [***list of third parties (e.g., system owner, project management, etc.)***] given [***limitations on the evidence of origin (e.g., access authorization, formal access authorization, need-to-know, etc.)***]. The information system security controls shall be able to relate the identity of user, level/category of information and [***list of attributes (e.g., user ID, authorized, labels authorized, permission attributes)***] of the originator of the information and the [***list of information fields (e.g., header information, IP addresses, etc.)***] of the information to which the evidence applies.

CO-2 PROOF OF RECEIPT

The information system security controls shall be able to generate evidence of receipt for received [***list of information types (e.g., Confidential/Secret, Secret RD, Confidential RD, Secret RD 1-13, etc)***] at the request of the originator, recipient, ISSO, or [***list of third parties (e.g., system owner, ISSM, project management, etc.)***] and provide a capability to verify the evidence of origin of information to the originator, recipient, or [***list of third parties (e.g., system owner, project management, etc.)***] given [***limitations on the evidence of origin (e.g., access authorization, formal access authorization, need-to-know, etc.)***]. The information system security controls shall be able to relate the [***list of attributes (e.g., user ID, authorized, labels authorized, permission attributes))***] of the recipient of the information, and the [***list of information fields (e.g., header information, IP addresses, etc.)***] of the information to which the evidence applies.

c. Cryptographic Support.

The PCSP must require each operating unit to implement the Cryptographic Support controls listed in Table 7 pertaining to the indicated protection index for all national security systems under their responsibility. These controls address the operational use and management of cryptographic keys when the information system implements cryptographic functions.

Table 7. Cryptographic Support Controls

Cryptographic Support Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
CS-1	Cryptographic Key Establishment and Management	CS-1	CS-1	CS-1	CS-1	CS-1	CS-1	CS-1
CS-2	Cryptographic Operation	CS-2	CS-2	CS-2	CS-2	CS-2	CS-2	CS-2

CS-1 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

When cryptography is required and used within the information system for other than telecommunications, the information system security controls shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. The requirements in DOE Manual 205.1-3, *Telecommunications Security Manual,* must be implemented for telecommunications systems. If cryptographic keys are not used, this should be stated in the SSP.

CS-2 CRYPTOGRAPHIC OPERATION

When cryptography is required and used within the information system for other than telecommunications ,the information system security controls shall perform [***list of cryptographic operations (e.g., password encryption, e-mail encryption, etc.)***] in accordance with [***specify the cryptographic algorithms*** *(e.g., AES, Triple-DES, etc.)*] and [*specify the cryptographic key sizes*] that meet [*list of standards (e.g., FIPS 140-2, etc.)*]. The requirements in DOE M 205.1-3, *Telecommunications Security Manual,* must be implemented for telecommunications systems. If cryptographic keys are not used this should be stated in the SSP.

d. User Data Protection.

The PCSP must require each operating unit to implement the User Data Protection controls listed in Table 8 pertaining to the indicated protection index for all national security systems under their responsibility. These controls address user data within the information system, during import, export, and storage as well as security attributes related to user data.

Table 8. User Data Protection Controls

User Data Protection Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
DP-1	Complete Access Control	DP-1	DP-1	DP-1	DP-1	DP-1	DP-1	DP-1
DP-2	Security Attribute Based Access Control	DP-2	DP-2	DP-2	DP-2	DP-2	DP-2	DP-2
DP-3	Basic Data Authentication	DP-3	DP-3	DP-3	DP-3	DP-3	DP-3	DP-3
DP-4	Export of User Data Without Security Attributes	N/A	N/A	N/A	N/A	DP-4	DP-4	DP-4
DP-5	Export of User Data With Security Attributes	N/A	N/A	N/A	N/A	DP-5	DP-5	DP-5
DP-6	Subset Information Flow Control	DP-6 (1)	DP-6 (1)	DP-6 (1)	DP-6 (1)	DP-6 (2)	DP-6 (2)	DP-6 (2)
DP-7	Simple Security Attributes	DP-7	DP-7	DP-7	DP-7	N/A	N/A	N/A
DP-8	Hierarchical Security Attributes	N/A	N/A	N/A	N/A	DP-8	DP-8	DP-8
DP-9	Import of User Data Without Security Attributes	DP-9	DP-9	DP-9	DP-9	DP-9(1)	DP-9(1)	DP-9(1)
DP-10	Import of User Data With Security Attributes	N/A	N/A	N/A	N/A	DP-10	DP-10	DP-10
DP-11	Full Residual Information Protection	DP-11	DP-11	DP-11	DP-11	DP-11 (1)	DP-11 (1)	DP-11 (1)
DP-12	Stored Data Integrity Monitoring and Action	DP-12	DP-12	DP-12	DP-12	DP-12	DP-12	DP-12

DP-1 COMPLETE ACCESS CONTROL

The information system security controls shall enforce the Discretionary Access Control (DAC) security policy based on access authorization and need-to-know on all subjects acting on behalf of users, all named objects, and all operations among subjects and objects covered by the DAC security policy. The DAC security policy shall apply to all operations between any object and subject within the information system. Any

named object that is not controlled by the DAC security policy must be justified in the SSP.

DP-2 SECURITY ATTRIBUTE BASED ACCESS CONTROL

The information system security controls shall enforce the DAC security policy to objects based on the user identity and group memberships associated with a subject; and the following access control attributes associated with an object: [***list access control attributes (e.g., identity of users, subjects, or objects; time restrictions; group membership)***]. The access control attributes must provide the ability to associate allowed or denied operations with one or more user identities; the ability to associate allowed or denied operations with one or more group identities; and defaults for allowed or denied operations.

In addition to the rules specified in DP-1, the information system security controls shall enforce [***a set of rules specifying the DAC policy***] to determine if an operation among controlled subjects and controlled objects is allowed. For each operation, there shall be a DAC rule, or rules, that use:

- The permission attributes where the user identity of the subject matches a user identity specified in the access control attributes of the object;
- The permission attributes where the group membership of the subject matches a group identity specified in the access control attributes of the object; and
- The default permission attributes specified in the access control attributes of the object when neither a user identity nor group identity matches.

The information system security controls shall explicitly authorize or deny access of subjects to objects based on the [***rules, based on security attributes, which explicitly authorize or deny access of subjects to objects (e.g., a specific privilege vector associated with a subject that always grants or denies access to specific objects)***].

In completing the rules above, the resulting mechanism must be able to specify access rules that apply to at least any single user. The mechanism must also support specifying access to the membership of at least any single group. Specification of these rules must be covered under DP-2 and DP-3. The PCSP or SSP must list the attributes that are used by the DAC policy for access decisions.

DP-3 BASIC DATA AUTHENTICATION

The information system security controls shall provide a capability to generate evidence (e.g., cryptographic checksum, fingerprint, message digest) that can be used as a guarantee of the validity of [***list of objects or information types (e.g., files, e-mail messages)***] and shall provide user or processes acting on behalf of users with the ability to verify evidence of the validity of the indicated information.

DP-4 EXPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

The information system security controls shall enforce the Mandatory Access Control (MAC) security policy and that devices used to export data without security attributes cannot be used to export data with security attributes unless the change in device state is performed manually and is auditable when exporting unlabeled user data, controlled under the MAC policy, outside the control of the information system.

Single-level Input/ Output devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process.

When data is exported in human-readable or printable form, the authorized administrator shall be able to specify the printable label that is assigned to the sensitivity label associated with the data; each print job shall be marked in accordance with DOE Classified Matter Protection and Control (CMPC) requirements.

When data is exported on removable media, the media must be marked in accordance with DOE CMPC requirements.

DP-5 EXPORT OF USER DATA WITH SECURITY ATTRIBUTES

The information system security controls shall enforce the Mandatory Access Control (MAC) security policy when exporting labeled user data, controlled under the MAC security policy when exporting, outside the control of the information system by exporting the user data with the user data's associated security attributes. The information system security controls shall ensure that the security attributes, when exported outside the control of the information system, are unambiguously associated with the exported user data and shall enforce the following rules when user data is exported from the control of the information system:

- When data is exported in a human-readable or printable form the authorized administrator shall be able to specify the printable label

that is assigned to the sensitivity label associated with the data; each print job shall be marked in accordance with DOE CMPC requirements.

- When data is exported on removable media, the media must be marked and protected in accordance with DOE CPMC requirements.
- Devices used to export data with security attributes cannot be used to export data without security attributes unless the change in device state is performed manually and is auditable.
- Devices used to export data with security attributes shall completely and unambiguously associate the security attributes with the corresponding data.

DP-6 SUBSET INFORMATION FLOW CONTROL

The information system security controls shall enforce access control policy based on protection index.

Control Enhancement (1): For PI-1 through PI-4, the DAC security policy shall be enforced on [***list of subjects (e.g., users, machines, processes), information (e.g., email, files, specified network protocols), and operations that cause controlled information to flow to and from controlled subjects covered by DAC***].

Control Enhancement (2): For PI-5 through PI-7, the MAC security policy shall be enforced on [***list of subjects (e.g., users, machines, processes), information (e.g., email, files, specified network protocols), and operations that cause controlled information to flow to and from controlled subjects covered by MAC***].

DP-7 SIMPLE SECURITY ATTRIBUTES

The information system security controls shall enforce the DAC security policy based on the following types of subject and information security attributes: [***list the minimum number and type of security attributes (e.g., user ID, group ID, file permission bits)***]. The information system security controls shall permit an information flow between a controlled subject and controlled information via a controlled operation if the security attribute-based relationship between the subject and object holds. The information system security controls may explicitly authorize or deny an information flow based on security attribute-based relationship between the subject and the object.

DP-8 HIERARCHICAL SECURITY ATTRIBUTES

The information system security controls shall enforce MAC security policy based on the sensitivity label of the subject and sensitivity label of the object containing the information. The sensitivity label of subjects and objects shall consist of a hierarchical level and a set of non- hierarchical categories. The information system security controls may explicitly authorize or deny an information flow based on [***rules, based on security attributes, which explicitly authorize or deny information flows***].

The information system security controls shall permit an information flow between a controlled subject and controlled information via a controlled operation, based on the ordering relationships between security attributes.

- If the sensitivity label of the subject (e.g., DOE Q clearance with additional Sigma authorizations) is greater than or equal to the sensitivity label of the object, then the flow of information from the object to the subject is permitted (a read operation);

- If the sensitivity label of the object is greater than or equal to the sensitivity label of the subject; then the flow of information from the subject to the object is permitted (a write operation); or

- If the sensitivity label of subject A is greater than or equal to the sensitivity label of subject B; then the flow of information from subject B to subject A is permitted. The information system security controls may explicitly authorize or deny an information flow based on [***rules, based on security attributes, which explicitly authorize or deny information flows***].

- The information system security controls may explicitly authorize or deny an information flow based on [***rules, based on security attributes, which explicitly authorize or deny information flows***].

DP-9 IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

When importing data from outside the control of the information system (via authorized means, such as removable media or document scanner), the information system security controls shall enforce the DAC security policy regardless of the security attributes associated with the data.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall enforce the MAC security policy when importing user data, controlled under the MAC security policy, from outside of the control of the information system. Devices used to import user data,

controlled under MAC security policy, without security attributes cannot be used to import data with security attributes unless the change in device state is performed manually and is auditable. Security attributes shall be assigned to data upon import to the information system.

DP-10 IMPORT OF USER DATA WITH SECURITY ATTRIBUTES

The information system security controls shall enforce the MAC security policy; wherein sensitivity labels consist of a hierarchical level and set of non-hierarchical categories when importing labeled user data from outside the control of the information system. The information system security controls shall ensure that the protocol used provides for the unambiguous association between security attributes and the labeled user data received and that interpretation of the security attributes of the imported labeled user data is as intended by the source of the user data. The information system security controls shall use the security attributes associated with the imported labeled user data and shall enforce the following rules when user data is imported from the control of the information system:

- Devices used to import data with security attributes cannot be used to import data without security attributes unless the change in device state is performed manually and is auditable.
- Devices used to import data with security attributes shall completely and unambiguously associate the security attributes with the corresponding data.

DP-11 FULL RESIDUAL INFORMATION PROTECTION

The information system security controls shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource.

Control Enhancement (1): For PI-5 through PI-7, the information systems security controls shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to all subjects.

DP-12 STORED DATA INTEGRITY MONITORING AND ACTION

The information system security controls shall monitor user data stored within the control of the information system for unauthorized modification and unauthorized deletion on all objects, based on the following [***user data attributes***]:

- When storing data to persistent storage, the information system shall make use of the underlying error detection/correction mechanisms of the media, and will detect and report failures on re-read.

- Where a particular persistent storage device does not innately provide an effective correction facility, the information system shall store data in such a way as to independently compute and validate an appropriate error detection check.

Upon detection of a data integrity error, the information system security control shall enter a description of the error in the audit log and issue an alarm.

e. Identification and Authentication.

The PCSP must require each operating unit to implement the User Data Protection controls listed in Table 9 pertaining to the indicated protection index for all national security systems under their responsibility. These controls address the ability of the information system to establish and verify a claimed user identity and its associated security attributes.

Table 9. Identification and Authentication Controls

Identification and Authentication Controls								
Control Identifier	Control Name	Protection Index						
		PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
IA-1	Authentication Failure Handling	IA-1	IA-1	IA-1	IA-1	IA-1	IA-1	IA-1
IA-2	User Attribute Definition	IA-2	IA-2	IA-2	IA-2	IA-2(1)	IA-2(1)	IA-2(1)
IA-3	Verification of Secrets	IA-3	IA-3	IA-3	IA-3	IA-3	IA-3	IA-3
IA-4	Timing of Authentication	IA-4	IA-4	IA-4	IA-4	IA-4	IA-4	IA-4
IA-5	Multiple Authentication Mechanisms	N/A	N/A	N/A	N/A	IA-5	IA-5	IA-5
IA-6	Re-authentication	N/A	N/A	N/A	N/A	IA-6	IA-6	IA-6
IA-7	Protected Authentication Feedback	IA-7	IA-7	IA-7	IA-7	IA-7	IA-7	IA-7
IA-8	Timing of Identification	IA-8	IA-8	IA-8	IA-8	N/A	N/A	N/A
IA-9	User Identification Before Any Action	N/A	N/A	N/A	N/A	IA-9	IA-9	IA-9
IA-10	User-subject DAC Binding	IA-10	IA-10	IA-10	IA-10	N/A	N/A	N/Av
IA-11	User-subject MAC Binding	N/A	N/A	N/A	N/A	IA-11	IA-11	IA-11

IA-1 AUTHENTICATION FAILURE HANDLING

The information system security controls shall detect when no more than five (5) consecutive unsuccessful authentication attempts occur related to the last successful session ***authentication*** for the indicated user. When the defined number of unsuccessful authentication attempts has been met or surpassed, the information system security controls shall inform the system administrator and disable the user account until it is unlocked by the administrator.

IA-2 USER ATTRIBUTE DEFINITION

The information system security controls shall maintain the security attributes of user identifier, group memberships, authentication data, and security-relevant role for individual users.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall maintain the security attribute of security clearances and formal access approvals for the individual users.

IA-3 VERIFICATION OF SECRETS

The information system security controls shall provide a mechanism to verify that secrets meet at least two-factor strong authentication mechanisms prior to granting access to systems and the information and resources managed by that system.

IA-4 TIMING OF AUTHENTICATION

The information system security controls shall allow [***list of information system security controls mediated actions (e.g., no actions)***] on behalf of the user to be performed before the user is authenticated. However, each user shall be successfully authenticated before allowing any other information system security controls mediated actions.

IA-5 MULTIPLE AUTHENTICATION MECHANISMS

The information system security controls may provide [***list of multiple authentication mechanisms (e.g., passwords; fingerprints; or smart cards)***] to support user authentication. Information system security controls shall authenticate any user's claimed identity according to the [***list the rules describing how the multiple authentication mechanisms provide authentication (e.g., the user must provide both a valid password and a fingerprint associated***

with the user identifier; or the user must provide a password and a smart card assigned to the user identifier)].

IA-6 RE-AUTHENTICATION

The information system security controls shall require re-authentication of the user under the conditions of unlocking as a result of locking.

IA-7 PROTECTED AUTHENTICATION FEEDBACK

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Note: Obscured feedback implies the information system security control does not produce a visible display of any authentication data entered by a user, such as through a keyboard (e. g., echo the password on the terminal). It is acceptable that some indication of progress be returned instead, such as a "period or an asterisk" returned for each character sent.

IA-8 TIMING OF IDENTIFICATION

The information system security controls shall allow [***list of information system security controls mediated actions (e.g., no actions)***] on behalf of the user to be performed before the user is identified.

IA-9 USER IDENTIFICATION BEFORE ANY ACTION

The information system security controls shall require each user to identify itself before allowing any other information system security controls mediated actions on behalf of that user.

IA-10 USER-SUBJECT DAC BINDING

The information system security controls shall associate the following user security attributes with subjects acting on behalf of that user: the user identity that is associated with auditable events; the user identity or identities that are used to enforce the DAC security policy; and the group membership or memberships used to enforce the DAC security policy.

IA-11 USER-SUBJECT MAC BINDING

The information system security controls shall associate the user security attribute of sensitivity label, consisting of a hierarchical level and a set of non-hierarchical categories, used to enforce the MAC security policy

which with subjects acting on behalf of that user. The information system security controls shall enforce the following additional rule on the initial association of user security attributes with subjects acting on behalf of that user: the sensitivity label associated with a subject shall be within the clearance range, and the clearance level and formal access approvals of the user.

f. Security Management.

The PCSP must require each operating unit to implement the Security Management controls listed in Table 10 pertaining to the indicated protection index for all national security systems under their responsibility. These controls address management of security attributes, information system security controls data and functions, and different management roles and their interaction.

Table 10. Security Management Controls

Security Management Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
MT-1	Management of Security Functions Behavior	MT-1	MT-1	MT-1	MT-1	MT-1	MT-1	MT-1
MT-2	Management of Security Attributes	MT-2	MT-2	MT-2	MT-2	MT-2(1)	MT-2(1)	MT-2(1)
MT-3	Static Attribute Initialization	MT-3	MT-3	MT-3	MT-3	MT-3(1)	MT-3(1)	MT-3(1)
MT-4	Management of Security Data	MT-4	MT-4	MT-4	MT-4	MT-4(1)	MT-4(1)	MT-4(1)
MT-5	Revocation	MT-5	MT-5	MT-5	MT-5	MT-5(1)	MT-5(1)	MT-5(1)
MT-6	Restrictions on Security Roles	MT-6	MT-6	MT-6	MT-6	MT-6(1)	MT-6(1)	MT-6(1)

MT-1 MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR

The information system security controls shall restrict the ability to determine or modify the behavior of, disable, and enable the functions [***list of security functions (e.g., management functions that relate to access control, accountability and authentication controls, controls over availability)***] to ISSOs and authorized system administrators.

MT-2 MANAGEMENT OF SECURITY ATTRIBUTES

The information system security controls shall enforce the DAC security policy to restrict the ability to modify the security attributes [***list of access control attributes (e.g., the groups to which a user belongs and the rights, such as read, write, and execute belonging to a role or user.)***]. The information system security controls shall ensure that only SSP-defined values are accepted for security attributes. The PCSP or SSP must state the components of the access rights that may be modified, must state any restrictions that may exist for a type of authorized user, and the components of the access rights that the user is allowed to modify. The ability to modify access rights must be restricted in that a user having access rights to a named object does not have the ability to modify those access rights unless granted the right to do so.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall enforce the MAC security policy to restrict the ability to modify the security attributes sensitivity label associated with an object to the ISSO and ***users*** authorized ***by the ISSO.*** The information system must immediately notify the user of each change in the security level or compartment associated with that user during an interactive session.

MT-3 STATIC ATTRIBUTE INITIALIZATION

The information system security controls shall enforce the DAC security policy to provide restrictive default values for security attributes that are used to enforce the DAC security policy.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall enforce the MAC security policy to provide restrictive default values for security attributes that are used to enforce the MAC security policy.

The information system security controls shall allow the ISSO and users authorized by the ISSO to specify alternative initial values to override the default values when an object or information is created.

MT-4 MANAGEMENT OF SECURITY DATA

The information system security controls shall restrict the ability to create, delete, and clear the audit trail and to modify and observe the set of audited events to ISSOs and authorized system administrators. The information system security controls shall restrict the ability to initialize the authentication data and initialize and modify the user security attributes, other than authentication data, to authorized system

administrators. The information system security controls shall restrict the ability to modify the authentication data to authorized system administrators and those users explicitly authorized to modify their own authentication data (e.g., passwords).

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall restrict the ability to modify the information system and object representation of time to ISSOs and authorized system administrators.

MT-5 REVOCATION

The information system security controls shall restrict the ability to revoke security attributes associated with the users within the information system's control to the ISSO and authorized system administrators. The information system security controls shall enforce the immediate revocation of security-relevant authorizations (e.g., next login, next attempt to open the file, within a fixed time). Upon revocation of security-relevant authorizations (e.g., disable subject) the system must [*list of authorized actions (e.g., reassign ownership of objects, disable access to objects)*] to ensure control of objects owned by subject. The information system security controls shall restrict the ability to revoke the security attributes associated with objects within the information system's control to users authorized to modify the security attributes by DAC or MAC security policies. The information system security controls shall enforce the access rights associated with an object when an access check is made.

Control Enhancement (1): For PI-5 through PI-7, the rules of the MAC security policy (DP-6) are enforced on all future operations.

MT-6 RESTRICTIONS ON SECURITY ROLES

The information system security controls shall be able to associate users with roles and shall maintain the roles of ISSO, authorized system administrator, and users explicitly authorized by the DAC security policy to modify object security attributes and their own authentication data (e.g., passwords). The information system security controls shall ensure that the conditions of [*list conditions for the different roles (e.g., least privilege for each use to perform the assigned role; a user assigned as an ISSO cannot also be assigned the system administrator role and vice versa)*] are satisfied.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall also maintain the role of users authorized by the MAC security policy to modify object security attributes.

g. Protection of the Information System Control Data.

The PCSP must require each operating unit to implement the Protection of the Information System Security Control Data listed in Table 11 pertaining to the indicated protection index for all national security systems under their responsibility. These controls ensure the mechanisms that provide the integrity and security functions of the information system security controls operate as designed. The focus is on information system control data protection rather than user data protection.

Table 11. Protection of the Information System Security Controls

Protection of the Information System Security Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
PT-1	Information System Security Control Testing	PT-1	PT-1	PT-1	PT-1	PT-1	PT-1	PT-1
PT-2	Information System Security Control Data Transmission	PT-2	PT-2	PT-2	PT-2	PT-2(1)	PT-2(1)	PT-2(1)
PT-3	Information System Recovery	PT-3	PT-3	PT-3	PT-3	PT-3	PT-3	PT-3
PT-4	Replay Detection	N/A	N/A	N/A	N/A	PT-4	PT-4	PT-4
PT-5	Non-bypassability of the Security Policy	PT-5	PT-5	PT-5	PT-5	PT-5	PT-5	PT-5
PT-6	Domain Separation	PT-6	PT-6	PT-6	PT-6	PT-6(1)	PT-6(1)	PT-6(1)
PT-7	Reliable Time Stamps	PT-7	PT-7	PT-7	PT-7	PT-7	PT-7	PT-7
PT-8	Fail Secure	PT-8	PT-8	PT-8	PT-8	PT-8	PT-8	PT-8

PT-1 INFORMATION SYSTEM SECURITY CONTROL TESTING

The information system controls shall run a suite of self-tests (e.g., hardware page protection, sample communications across a network to ensure receipt, and verifying the behavior of specific controls) during initial start-up, periodically during normal operation, or at the request of the authorized user and [***list other conditions under which self test should occur (e.g., recovery from failed condition/event)***] to demonstrate the correct operation of the information system security controls.

PT-2 INFORMATION SYSTEM SECURITY CONTROL DATA TRANSMISSION

The information system security controls shall protect all information system security control data transmitted from the information system to a remote trusted IT product from unauthorized disclosure during transmission.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall protect information system security control data from disclosure when it is transmitted between separate parts (components) of the information system.

PT-3 INFORMATION SYSTEM RECOVERY

The organization employs manual or automated mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

PT-4 REPLAY DETECTION

The information system security controls shall detect replay for [***list of identified entities (e.g., messages, service requests, service responses, and user sessions)***] and shall perform [***list of specific actions (e.g., ignoring the replayed entity, requesting confirmation of the entity from the identified source, and terminating the subject from which the replayed entity originated)***] when replay is detected.

PT-5 NON-BYPASSABILITY OF THE SECURITY POLICY

The information system security controls shall ensure that the information system security policy enforcement functions are invoked and succeed before each function within the information system's control is allowed to proceed.

PT-6 DOMAIN SEPARATION

The un-isolated portion of the information system security controls shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects and shall enforce separation between the security domains of subjects under the control of the information system.

The information system security controls shall maintain the part of the information system security controls related to the DAC security policy in a security domain for their own execution that protects them from interference and tampering by the remainder of the information system's

controls and by subjects untrusted with respect to those DAC security policy.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall maintain the part of the information system security controls related to the DAC and MAC security policies in a security domain for their own execution that protects them from interference and tampering by the remainder of the information system security controls and by subjects untrusted with respect to those DAC or MAC security policies.

PT-7 RELIABLE TIME STAMPS

The information system security controls shall be able to provide reliable time stamps for its own use.

PT-8 FAIL SECURE

The information system shall fail to a "secure" state, defined in the SSP, in which the security functions of the data are consistent and the security functions continue correct enforcement of the security policy. The SSP shall also specify those situations in which audit is desired and feasible from the "secure" state.

Failures in the security function may include "hard" failures, which indicate an equipment malfunction and may require maintenance, service or repair of the security function. Failures in the security function may also include recoverable "soft" failures (e.g., failure of the integrity of information system security control data, initialization or resetting of the security function, etc.).

h. Resource Utilization.

The PCSP must require each operating unit to implement the Resource Utilization controls listed in Table 12 pertaining to the indicated protection index for all national security systems under their responsibility. These controls support the availability of required resources.

Table 12. Resource Utilization Controls

Resource Utilization Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
RU-1	Quotas	N/A	N/A	RU-1	RU-1(1)	RU-1(1)	RU-1(1)	RU-1(1)

RU-1 QUOTAS

The information system security controls shall enforce **maximum** quotas of [*list of controlled resources (e.g., file servers, disk drives, print spoolers, etc.)*] that an individual user, defined group of users, subjects can use simultaneously and/or over a specified period of time.

Control Enhancement (1): For PI-4 through PI-7, the information system security controls shall enforce **minimum** quotas of [*list of controlled resources (e.g., file servers, disk drives, print spoolers, etc.)*] that an individual user, defined group of users, or subjects can use simultaneously and/or over a specified period of time.

i. Information System Access.

The PCSP must require each operating unit to implement the Information System Access Controls listed in Table 13 pertaining to the indicated protection index for all national security systems under their responsibility. These controls are used to control the establishment of a user's session.

Table 13. Information System Access Controls

Information System Access Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
SA-1	Concurrent Sessions Limitations	SA-1	SA-1	SA-1	SA-1	SA-1	SA-1	SA-1
SA-2	Session Locking and Termination	SA-2	SA-2	SA-2	SA-2	SA-2	SA-2	SA-2
SA-3	Default Access Banners	SA-3	SA-3	SA-3	SA-3	SA-3	SA-3	SA-3
SA-4	Information System Access History	SA-4	SA-4	SA-4	SA-4	SA-4	SA-4	SA-4
SA-5	Deny Session Establishment	SA-5	SA-5	SA-5	SA-5	SA-5	SA-5	SA-5

SA-1 CONCURRENT SESSIONS LIMITATIONS

The information system security controls the number of concurrent sessions for any user to [*Assignment: organization-defined number* of *sessions*].

SA-2 SESSION LOCKING AND TERMINATION

The information system security controls prevents further access to the system by initiating a session lock after [***Assignment: organization-defined time period (e.g., 15 minutes) of inactivity***] and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The information system automatically terminates a remote session after [***Assignment: organization-defined time period (e.g., 15 minutes after session lock period initiates)***] of inactivity.

SA-3 DEFAULT ACCESS BANNERS

The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and (ii) that system usage may be audited, intercepted, monitored, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. (See EN-12 for the sample warning text.)

The notification message and remains on the screen until the user takes explicit actions to log on to the information system.

SA-4 INFORMATION SYSTEM ACCESS HISTORY

The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

SA- 5 DENY SESSION ESTABLISHMENT

The information system security controls shall be able to deny session establishment based on [***list attributes (e.g., user's identity, clearance level, integrity level, membership in a role)***].

j. Trusted Path/Channels.

The PCSP must require each operating unit to implement the Trusted Path/Channels controls listed in Table 14 pertaining to the indicated protection indices for all national security systems under their responsibility. These controls are used to provide secure communication path between users

and the information system security controls and a trusted channel between the information system security controls and other trusted IT products.

Table 14. Trusted Path/Channels Controls

Trusted Path/Channels Controls								
Control Identifier	Control Name	Protection Index						
		PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
TP-1	Trusted Path	TP-1	TP-1	TP-1	TP-1	TP-1	TP-1	TP-1

TP-1 TRUSTED PATH

The information system security controls shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. The information system security controls shall require the use of the trusted path for initial user authentication and [***other services for which trusted path is required (e.g., transmission authorizations, authentication to resources, etc.)***] and shall permit the information system security controls, local users, or remote users to initiate communication via the trusted path.

7. OPERATIONAL CONTROLS.

The PCSP must require each operating unit to implement the Operational Controls listed in Table 15 pertaining to the indicated protection index for all national security systems under their responsibility. Operational controls are intended to be implemented within the environment in which the information system resides through processes, procedures, or other information systems. Operational controls were constructed for those objectives that rely on physical protection and security processes and for those objectives that are solely security operational issues.

NOTE: The control identifier appears in the following tables to indicate that the control listed on the left must be implemented for the protection index across the top. The parenthetical numbers represent additional control enhancement described in the control statement. Where bolded and italicized items are listed in the control statement, the PCSP or SSP developer must provide the information identified in the ***italicized*** clause to describe the implementation.

Table 15. Operational Controls

Operational Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
EN-1	Malicious Access	EN-1	EN-1	EN-1	EN-1	EN-1	EN-1	EN-1
EN-2	Management of User Identifiers and Authenticators	EN-2	EN-2	EN-2	EN-2	EN-2	EN-2	EN-2
EN-3	Information Availability	EN-3	EN-3	EN-3	EN-3	EN-3	EN-3	EN-3
EN-4	Purging	EN-4	EN-4	EN-4	EN-4	EN-4	EN-4	EN-4
EN-5	Covert Channels	N/A	N/A	N/A	N/A	EN-5	EN-5	EN-5
EN-6	Hardware and Software Examination	N/A	EN-6	EN-6	EN-6 (1)	EN-6 (1)(2)	EN-6 (1)(2)	EN-6 (1)(2)
EN-7	Forensics	EN-7	EN-7	EN-7	EN-7	EN-7	EN-7	EN-7
EN-8	Intrusion Detection	EN-8	EN-8	EN-8	EN-8	EN-8	EN-8	EN-8
EN-9	Information System Interface	EN-9	EN-9	EN-9	EN-9	EN-9	EN-9	EN-9
EN-10	Marking	EN-10	EN-10	EN-10	EN-10	EN-10	EN-10	EN-10
EN-11	Interconnected Environment	EN-11	EN-11	EN-11	EN-11	EN-11	EN-11	EN-11
EN-12	User Notification	EN-12	EN-12	EN-12	EN-12	EN-12	EN-12	EN-12
EN-13	Need-to-Know	EN-13	EN-13	EN-13	EN-13	EN-13	EN-13	EN-13
EN-14	Physical Security	EN-14	EN-14	EN-14	EN-14	EN-14	EN-14	EN-14
EN-15	Physical Access Protection	EN-15	EN-15	EN-15	EN-15	EN-15	EN-15	EN-15
EN-16	Environmental Protection	EN-16	EN-16	EN-16	EN-16	EN-16	EN-16	EN-16
EN-17	Information Protection	EN-17	EN-17	EN-17	EN-17	EN-17	EN-17	EN-17
EN-18	System Recovery	EN-18	EN-18	EN-18	EN-18	EN-18	EN-18	EN-18
EN-19	Media and Component Review	EN-19	EN-19	EN-19	EN-19	EN-19	EN-19	EN-19

Operational Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
EN-20	User Access Rights and Privileges	EN-20	EN-20	EN-20	EN-20	EN-20	EN-20	EN-20
EN-21	Security Roles	EN-21	EN-21	EN-21	EN-21	EN-21	EN-21	EN-21
EN-22	Two-Person Rule	N/A	N/A	N/A	N/A	EN-22	EN-22	EN-22
EN-23	User Training	EN-23	EN-23	EN-23	EN-23	EN-23	EN-23	EN-23
EN-24	User Clearance	EN-24 (1)	EN-24 (2)	EN-24 (1)	EN-24 (2)	EN-24 (2)	EN-24 (2)	EN-24 (2)
EN-25	National Security Systems Workstations	EN-25	EN-25	EN-25	EN-25	EN-25	EN-25	EN-25

EN-1 MALICIOUS ACCESS

Information system security controls shall be implemented to detect, deter, and respond to malicious actions by authenticated users.

EN-2 MANAGEMENT OF USER IDENTIFIERS AND AUTHENTICATORS

Authentication credentials shall be protected from unauthorized access during creation, use, and handling. Authenticated user information system access shall be disabled when the user leaves the sponsoring organization, Access Authorization is terminated, loses authorized access (for cause, changes in organization, etc), or upon information system detection of attempts to bypass security. Prior to reuse of an authenticated user identifier, all previous access rights and privileges (including file accesses for that user identifier) shall be removed from the information system. Authenticated user access, contact information, rights, and privileges, to include sponsor, Access Authorization, need-to-know, means for off line contact, mailing address, shall be validated annually.

EN-3 INFORMATION AVAILABILITY

Capabilities and resources shall be provided to allow the information system user to perform data backup at the user's discretion. User and information system data shall be available, or restorable, to meet mission availability requirements. Periodic checking of backup inventory and testing of the ability to restore information shall be accomplished to validate mission availability requirements are met. The organization shall conduct backups of user-level and system-level information (including

system state information) contained in the information system [*Assignment: organization-defined frequency*].

EN-4 PURGING

The information system components and removable media shall be purged before the items can be reused in another system environment with the same or different accreditation level as the original system components or removable media.

All information system components and removable media shall be purged, using Senior DOE Management approved procedures, prior to release for use at a lower classification level, at a lower level of consequence, or outside the information system boundary.

EN-5 COVERT CHANNELS

The information system must be reviewed to identify obvious covert channels.

EN-6 HARDWARE AND SOFTWARE EXAMINATION

Information system hardware and software components shall be examined for security impacts to the information system before use.

Control Enhancement (1): For PI-4 through PI-7, information system hardware components shall be examined to validate the chip sets and boards are from the manufacturer before use. Information system software components shall be examined and tested to determine if the software conforms to security relevant controls as documented by the system owner and contains no malicious code before use.

Control Enhancement (2): For PI-5 through PI-7, information system hardware components shall be examined by manufacturer diagnostics to confirm the information system chip sets and boards function as expected before use. Information system software components shall be examined and tested to determine if controls can be bypassed before use.

EN-7 FORENSICS

Procedures shall be established and documented to ensure the identification, collection, and preservation of data (at the system and network level) needed to analyze and reconstruct events resulting from penetration attempts, penetrations, and on-going cyber attacks and/ or failures.

EN-8 INTRUSION DETECTION

The site and network (when applicable) environment shall provide the ability to detect (i.e., using methods readily available on the Internet to attack known vulnerabilities) and sophisticated attacks on the network, network components, and hosts from inside or outside the site, including measures to detect and respond to unauthorized attempts to penetrate or deny use.

EN-9 INFORMATION SYSTEM INTERFACE

The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external connection, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. The information system denies information flow by default and allows information flow by exception (i.e., deny all, permit by exception). The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

EN-10 MARKING

Each information system, visual display, and output device shall be marked in accordance with DOE Manual 470.4-4, Section 2.

EN-11 INTERCONNECTED ENVIRONMENT

The information system must provide the ability to specify and manage user access rights to the information system and data resources (i.e. access authorization through the network), supporting the organization's security policy for access control.

EN-12 USER NOTIFICATION

All users shall be notified that they are subject to being monitored, recorded, and audited through the use of the following approved warning text.

WARNINGWARNING**WARNING**WARNING**

This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY.

WARNINGWARNING**WARNING**WARNING**

Explicit acknowledgement of the warning by the user is required before granting the user access to system resources.

EN-13 NEED-TO-KNOW

Prior to their first access to information, each user's need-to-know shall be formally authorized by management, the data owner, or the data-steward.

EN-14 PHYSICAL SECURITY

Access controls shall ensure that personnel granted unescorted physical access to the information, the information system, or human readable media have the appropriate access authorization, formal access approval, and need-to-know. Physical attack, which might compromise security, on those parts of the information system critical to security shall be deterred and detected.

EN-15 PHYSICAL ACCESS PROTECTION

The information system shall be protected by being constantly attended and under the control of a person that possesses proper access authorization, formal access approval, and need-to-know, or by physical protection, as prescribed for the classification level and category of the information, to restrict access to those with appropriate clearance, formal access approvals, and need-to-know.

The information system shall be protected by default setting of disabled/closed, with all ports and/or devices capable of writing to removable or external media being protected from unauthorized modification or use by [***describe software and/or hardware means used***

to prevent unauthorized use or modification of all ports and/or devices capable of writing to removable or external media (e.g., software such as Sanctuary, etc.)]. When this protection is implemented by software, the named object must be listed in DP-1 and access control rules described in DP-2.

EN-16 ENVIRONMENTAL PROTECTION

The information system environment shall be capable of physically protecting the information system and components stored in a remote location by signaling the occurrence of fire, flood, power loss, and environmental control failures that might adversely affect information system operations.

EN-17 INFORMATION PROTECTION

Information protection shall be required whenever national security information is to be transmitted through components or areas where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media. One or more of the following methods approved through the Senior DOE Management PCSP for the level and category of information must be used to protect the information in transit [***i.e., information distributed only within an area approved for open storage of the information; National Security Agency (NSA) approved Type I encryption mechanisms; DOE approved encryption mechanisms; or DOE approved Protected Transmission Systems***].

EN-18 SYSTEM RECOVERY

All remote terminal access must be monitored and controlled when used for system recovery operations.

EN-19 MEDIA AND COMPONENT REVIEW

All media (paper, disks, zip drives, removable disk drives, etc.) shall be reviewed by an authorized derivative classifier for sensitivity and properly marked before release outside the system boundary.

EN-20 USER ACCESS RIGHTS AND PRIVILEGES

Each user's access rights and privileges shall be based on the least privilege principle and authorized by the ISSO or user(s) authorized by the ISSO prior to the user's first access to the information system.

EN-21 SECURITY ROLES

The same person must not perform the functions of the ISSO and the system administrator. Other roles involved with security administration, such as DBMS administration, must not performed by the same people performing the ISSO and system administrator roles.

EN-22 TWO-PERSON RULE

The ISSO and system administrator shall be present when audit parameters or audit file contents are modified.

EN-23 USER TRAINING

All authenticated users shall be trained to understand applicable information system use policies, the approved use of the information system, the vulnerabilities inherent in the operation of the information system, and their cyber security responsibilities.

EN-24 USER CLEARANCE

All users (including privileged users) shall possess a current Access Authorization prior to their first access to the information system.

Control Enhancement (1): For PI-1 and PI-3, all users shall, at a minimum, possess a current "L" Access Authorization.

Control Enhancement (2): For PI-2 and PI-4 through PI-7, all users shall, at a minimum, possess a current "Q" Access Authorization.

EN-25 NATIONAL SECURITY SYSTEM WORKSTATIONS

Workstations shall be prohibited from reading from, or writing to, removable media without appropriate security controls, including system-level intervention to permit unique read/write events. The security controls and unique read/write events shall be documented in the security plan. Additionally, diskless workstations not located within an area approved for "open storage" of classified information shall not contain non-volatile memory (other than simple BIOS).

8. ASSURANCE CONTROLS.

Assurance controls are intended to be implemented through: (1) actions taken by system owners (developers and implementers) of security controls to use state-of-the-practice design, development, and implementation techniques and methods; and (2) actions taken

by security control certifiers during the Certification and Accreditation (C&A) process to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Assurance considerations related to developers and implementers of security controls are addressed in this Manual. The assurance philosophy is to provide assurance based upon an evaluation (active investigation) of the information system by checking the validity of the documentation and the resulting information system by certifiers with increasing emphasis on scope, depth, and rigor.

NOTE: The control identifier appears in the following tables to indicate that the control listed on the left must be implemented for the protection index across the top. The parenthetical numbers represent additional control enhancement described in the control statements.

a. Configuration Management.

The PCSP must require each operating unit to implement the Configuration Management assurance controls listed in Table 16 pertaining to the indicated protection index for all national security systems under their responsibility. These controls are used to ensure the integrity of the information system is preserved by requiring discipline and control in the process of refinement and modification of the information system and other related information. Configuration Management provides assurance that the information system and documentation used to evaluate the information system reflect the same requirements.

Table 16. Configuration Management Controls

Configuration Management Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
CM-1	Configuration Management System	CM-1	CM-1	CM-1	CM-1 (1)	CM-1 (1)	CM-1 (1)	CM-1 (1)
CM-2	Configuration Management Documentation	CM-2	CM-2	CM-2	CM-2 (1)	CM-2 (1)	CM-2 (1)	CM-2 (1)

CM-1 CONFIGURATION MANAGEMENT SYSTEM

The system owner shall provide a reference identifier for the information system, use a Configuration Management (CM) system, and provide CM documentation.

The reference identifier for the information system shall be unique to each version of the information system and the information system shall be labeled with its reference. The CM system shall uniquely identify all configuration items. The CM documentation shall include a configuration list that describes the configuration items that comprise the information system and the method used to uniquely identify the configuration items.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for content.

The CM documentation shall include a CM plan that describes how the CM system is used. The CM system shall provide measures such that only authorized changes are made to configuration items. The C&A process shall demonstrate that the CM system is operating in accordance with the plan and documentation shows that all configuration items have been and are being effectively maintained under the CM system.

Control Enhancement (1): For PI-4 through PI-7, the CM documentation shall include an acceptance plan that describes the procedures used to accept modified or newly created configuration items. The CM system shall support the generation of the information system, provide an automated means by which only authorized changes are made to the information system and CM implementation representation, and describe the automated tools used in the CM system.

CM-2 CONFIGURATION MANAGEMENT DOCUMENTATION

The system owner shall provide CM documentation. The CM documentation shall show that the CM system, as a minimum, tracks the following: The information system implementation representation, design documentation, functional and security test documentation, user documentation, administrator documentation, and CM documentation (e.g., version and change log). The CM documentation shall describe how the configuration items are tracked by the CM system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for the content.

Control Enhancement (1): For PI-4 through PI-7, the CM documentation shall show that the CM system tracks security flaws.

b. Delivery and Operations.

The PCSP must require each operating unit to implement the Delivery and Operations assurance controls listed in Table 17 pertaining to the indicated protection index for all national security systems under their responsibility.

These controls are used to define the measures, procedures, and standards concerned with secure delivery, installation, and operational use of the information system ensuring that the security protection offered by the information system is not compromised during transfer, installation, start-up, and operation.

Table 17. Delivery and Operations Controls

Delivery and Operations Controls								
Control Identifier	Control Name	Protection Index						
		PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
DO-1	Delivery Procedures	DO-1	DO-1	DO-1	DO-1	DO-1	DO-1	DO-1
DO-2	Installation, Generation, and Startup Procedures	DO-2	DO-2	DO-2	DO-2	DO-2	DO-2	DO-2

DO-1 DELIVERY PROCEDURES

The system owner shall document procedures for delivery of the information system or parts of it to the user and shall use the delivery procedures. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the information system or updates to the user's site.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for the content.

DO-2 INSTALLATION, GENERATION, AND STARTUP PROCEDURES

The system owner shall document procedures necessary for the secure installation, generation, and startup of the information system. The documentation shall describe the steps necessary for secure installation, generation, and start-up of the information system. The documentation shall confirm that the information provided meets all requirements for content.

The certifier, during the C&A process, shall determine that the installation, generation and startup procedures result in a secure configuration.

Note: The required documentation depends on the way that the information system is generated and installed. For example, the generation of the information system from source code may be done at the development site, in which case the required documentation would be considered part of the design documentation. If some part of the information system generation is done by the system administrator, it would be part of the administrative guidance. Similar circumstances would apply to both installation and startup procedures.

c. Development.

The PCSP must require each operating unit to implement the Development assurance controls listed in Table 18 pertaining to the indicated protection index for all national security systems under their responsibility. These controls are used to define the information system security controls at various levels of detail and provide information to help the certifier determine whether the controls have been properly implemented.

Table 18. Development Controls

Development Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
DV-1	Correspondence Demonstration	DV-1	DV-1	DV-1 (1)	DV-1 (1)	DV-1 (1)	DV-1 (1)	DV-1 (1)
DV-2	Implementation of the Information System Controls	N/A	N/A	N/A	N/A	DV-2	DV-2	DV-2
DV-3	Information System Security Policy Model	N/A	N/A	N/A	N/A	DV-3	DV-3	DV-3

DV- 1 CORRESPONDENCE DEMONSTRATION

The system owner shall provide a functional specification for systems other than Commercial Off-the-Shelf (COTS) software. The functional specification shall provide the high-level design. The system owner shall provide the high-level design (HLD) of the information system security controls. The HLD shall be internally consistent; shall describe

the structure of the information system security controls in terms of subsystems; shall describe the security functionality provided by each subsystem of the information system security controls; shall identify any underlying hardware, firmware, and / or software required by the information system security controls with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software; shall identify all interfaces to the subsystems of the information system security controls; and shall identify which of the interfaces to the subsystems of the information system security controls are externally visible.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for content, shall determine that the functional specification is an accurate and complete representation of the information system security functional requirements, and determine that the high-level design is an accurate and complete description of the information system security functional requirements.

Control Enhancement (1): For PI-3 through PI-7, the HLD shall describe the purpose and method of use of all interfaces to the subsystems of the information system security controls, providing details of effects, exceptions, and error messages, as appropriate and shall describe the separation of the information system into security control-enforcing components and other subsystems.

DV-2 IMPLEMENTATION OF THE INFORMATION SYSTEM CONTROLS

The system owner shall provide the implementation representation for a selected subset of the information system security controls. The implementation representation shall unambiguously define the information system security controls to a level of detail such that the information system security controls can be generated without further design decisions. The implementation representation shall be internally consistent.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and presentation of evidence and determine that the least abstract information system security controls representation provided is an accurate and complete instantiation of the information system security functional requirements.

DV-3 INFORMATION SYSTEM SECURITY POLICY MODEL

The system owner shall provide an information system security policy model. The system owner shall demonstrate correspondence between the functional specification and the information system security policy model. The information system security policy model shall describe the rules and characteristics of all policies of the information system security policy that can be modeled and include a rationale that demonstrates that it is consistent and complete with respect to all policies of the information system security policy that can be modeled. The demonstration of correspondence between the information system security policy model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the information system security policy model.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

d. Guidance Documents.

The PCSP must require each operating unit to implement the Guidance Documents assurance controls listed in Table 19 pertaining to the indicated protection index for all national security systems under their responsibility. These controls are used to provide guidance to the system administrator and user for the secure operation of the information system that is understandable and complete.

Table 19. Guidance Documents Controls

Guidance Documents Controls								
Control Identifier	Control Name	Protection Index						
		PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
GD-1	Administrator Guidance	GD-1	GD-1	GD-1	GD-1	GD-1	GD-1	GD-1
GD-2	User Guidance	GD-2	GD-2	GD-2	GD-2	GD-2	GD-2	GD-2

GD-1 ADMINISTRATOR GUIDANCE

The system owner shall provide administrator guidance to system administrative personnel. The administrator guidance shall describe the administrative functions and interfaces available to the administrator of

the information system; shall describe how to administer the information system in a secure manner; shall contain warnings about functions and privileges that should be controlled in a secure processing environment; shall describe all assumptions regarding user behavior that are relevant to secure operation of the information system; shall describe all security parameters under the control of the administrator, indicating secure values as appropriate; shall describe each type of security relevant event relative to the administrative function that needs to be performed, including changing the security characteristics of entities under the control of the information system security controls; shall describe and be consistent with all other documentation supplied for evaluation; and shall describe all security requirements for the IT environment that are relevant to the administrator.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

GD-2 USER GUIDANCE

The system owner shall provide user guidance. The user guidance shall describe the functions and interfaces available to the non-administrative users of the information system; shall describe the use of user-accessible security functions provided by the information system; shall contain warnings about user accessible functions and privileges that should be controlled in a secure processing environment; shall clearly present all user responsibilities necessary for the secure operation of the information system, including those related to assumptions regarding user behavior found in the statement of the information system security environment; shall be consistent with all other documentation supplied for evaluation; and shall describe all security requirements for the IT environment that are relevant to the user.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

e. Life Cycle Support.

The PCSP must require each operating unit to implement the Life Cycle Support assurance controls listed in Table 20 pertaining to the indicated protection index for all national security systems under their responsibility. These controls are used to provide a well defined life-cycle model for the steps of the information system development, including flaw remediation procedures and policies, correct use of tools and techniques and the security measures used to protect the development environment.

Table 20. Life Cycle Support Controls

Life Cycle Support Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
LC-1	Identification of Security Measures	LC-1	LC-1	LC-1	LC-1	LC-1	LC-1	LC-1
LC-2	Flaw Remediation	N/A	N/A	LC-2	LC-2 (1)	LC-2 (1)	LC-2 (1)	LC-2 (1)
LC-3	Defined Life Cycle Model	N/A	N/A	N/A	LC-3	LC-3	LC-3	LC-3

LC-1 IDENTIFICATION OF SECURITY MEASURES

The system owner shall produce development security documentation. The development security documentation shall describe all physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the information system design and implementation in its development environment and shall provide evidence that these security measures are followed during the development and maintenance of the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and shall confirm that the security measures are being applied.

LC-2 FLAW REMEDIATION

Flaws in hardware or software may adversely affect the confidentiality, availability, or integrity of national security information. Flaws may be identified through a variety of means, such as vendor notifications, vulnerability analysis, or certification testing. The system owner shall document the flaw remediation procedures. The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the information system and shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to information system users. The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided as well as the status of finding a correction to the flaw and shall require that corrective actions be identified for each of the security flaws.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

The system owner shall establish a procedure for accepting and acting upon user reports of security flaws and requests for correction of those flaws and shall provide flaw remediation guidance addressed to information system users. The flaw remediation procedures documentation shall describe a means by which the system owner receives from information system users' reports and enquiries of suspected security flaws in the information system. The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to information system users and shall provide safeguards that any corrections to these security flaws do not introduce any new flaws. The flaw remediation guidance shall describe a means by which information system users report to the system owner any suspected security flaws in the information system and a means for verification that suspected security flaws are addressed.

Control Enhancement (1): For PI-4 through PI-7, the system owner shall designate one or more specific points of contact for user reports and inquiries about security issues involving the information system. The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw. The flaw remediation guidance shall describe a means by which information system users may register with the system owner, to be eligible to receive security flaw reports and corrections. The flaw remediation guidance shall identify the specific points of contact for all reports and inquiries about security issues involving the information system.

LC-3 DEFINED LIFE CYCLE MODEL

The system owner shall establish a life-cycle model to be used in the development and maintenance of the information system and shall provide life-cycle definition documentation. The life-cycle definition documentation shall describe the model used to develop and maintain the information system and the life-cycle model shall provide for the necessary control over the development and maintenance of the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

f. Tests.

The PCSP must require each operating unit to implement the Tests assurance controls listed in Table 21 pertaining to the indicated protection index for all national security systems under their responsibility. These controls are used to demonstrate that the information system security controls satisfies the information system security functional requirements.

Table 21. Tests Controls

Test Controls								
Control Identifier	Control Name	Protection Index						
		PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
TE-1	Test Coverage	TE-1	TE-1	TE-1(1)	TE-1(1)	TE-1(1)	TE-1(1)	TE-1(1)
TE-2	Testing	TE-2	TE-2	TE-2(1)	TE-2(1)	TE-2(1)	TE-2(1)	TE-2(1)

TE-1 TEST COVERAGE

The system owner shall provide evidence of the test coverage. The evidence of test coverage shall show the correspondence between the test identified in the test documentation and the information system security controls as described in the functional specification.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

Control Enhancement (1): For PI-3 through PI-7, the system owner shall provide an analysis of test coverage. The analysis of test coverage shall demonstrate the correspondence between the test identified in the test documentation and the information system security controls as described in the functional specification and between the information system security controls as described in the functional specification and the tests identified in the test documentation is complete.

TE- 2 TESTING

The system owner shall test the information system security controls and document the results. The system owner shall provide test documentation that consists of test plans, test procedure descriptions, expected test results, and the actual test results. The test plans shall

identify the security controls to be tested and describe the goal of the tests to be performed. The test procedures shall identify the test to be performed and describe the scenarios for testing each security function. The scenarios shall include any ordering dependencies on the results of other tests. The expected test results shall show the anticipated outputs from a successful execution of the tests. The test results from the system owner execution of the tests shall demonstrate that each tested security control behaved as specified. The system owner shall provide a suitable information system for testing and shall provide an equivalent set of resources to those that were used in the system owner's functional testing of the information system security controls.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content, shall select and test a subset of the information system security controls as appropriate to confirm that the information system operates as specified, and shall execute a sample of tests in the test documentation to verify the system owner test results.

Control Enhancement (1): For PI-3 through PI-7, the system owner shall provide the analysis of the depth of testing. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the information system security controls operates in accordance with its high-level design.

g. Vulnerability Assessment.

The PCSP must require each operating unit to implement the Vulnerability Assessment assurance controls listed in Table 22 pertaining to the indicated protection index for all national security systems under their responsibility. These controls are used to identify exploitable vulnerabilities introduced in development, operation, misuse, or incorrect configuration of the information system.

Table 22. Vulnerability Assessment Controls

Vulnerability Assessment Controls								
		Protection Index						
Control Identifier	Control Name	PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
VA-1	Vulnerability Analysis	VA-1	VA-1	VA-1	VA-1 (1)	VA-1 (1)	VA-1 (1)	VA-1 (1)
VA-2	Examination of Guidance	N/A	N/A	VA-2	VA-2 (1)	VA-2 (1)	VA-2 (1)	VA-2 (1)

VA-1 VULNERABILITY ANALYSIS

The system owner shall perform and document an analysis of the information system deliverables searching for obvious ways in which a user can violate the information system security policy. The system owner shall document the disposition of the obvious vulnerabilities and the documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and shall conduct penetration testing, building on the system owner vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

For PI-4 through PI-7, the system owner shall document the disposition of identified vulnerabilities. The documentation shall justify that the information system, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Control Enhancement (1): The certifier, during the C&A process, shall perform an independent vulnerabilities analysis; shall perform independent penetration testing based on the independent vulnerability analysis to determine the exploitability of additional identified vulnerabilities in the intended environment; and shall determine that the information system is resistant to penetration attacks performed by an attacker possessing a low attack potential.

Note: The certifier should consider the following with respect to the search for obvious flaws:

- Dependencies among functional components and potential inconsistencies in the strength of function among independent functions.
- Potential inconsistencies between the information system security policy and the functional specification.
- Potential gaps or inconsistencies in the HLD and potentially invalid assumptions about supporting hardware, software, or firmware required by the information system security controls.
- Potential gaps in the administrator guidance that enable the administrator to fail: a) to make effective use of information system security controls, b) to understands or take actions that need to be performed, c) to install and / or configure the information system

correctly, and d) to avoid unintended interactions among security functions. In particular, failure to describe all security parameters under the administrator's control and the effects of settings of those parameters.

- Potential gaps in user guidance that enable the user to fail to control functions and privileges as required maintaining a secure processing environment. Potential presence in the user guidance of information that facilitates exploitation of vulnerabilities.

- Open literature (e.g., CERT advisories, bug-trac mailing lists, etc.) which contain information on vulnerabilities on the information system security controls should be consulted.

VA-2 EXAMINATION OF GUIDANCE

The system owner shall provide guidance documentation. The guidance documentation shall identify all possible modes of operation of the information system (including operation following failure or operational error), their consequences and implications for maintaining secure operations. The guidance documentation shall be complete, clear, consistent, and reasonable; shall list all assumptions about the intended environment; and list all requirements for external security measures (including external procedural, physical and personnel controls).

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for content, shall repeat all configuration and installation procedures to confirm that the information system can be configured and used securely using only the supplied guidance documentation, and shall determine that the use of the guidance documentation allows all insecure states to be detected.

Control Enhancement (1): For PI-4 through PI-7, the system owner shall document an analysis of the guidance documentation that demonstrates the guidance documentation is complete.

The certifier, during the C&A process, shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the information system.

CHAPTER II. RESPONSIBILITIES

Senior DOE Management is responsible for ensuring the implementation of the DOE Cyber Security Program, this Manual, and the respective PCSPs under their purview.

1. DOE UNDER SECRETARIES, INCLUDING THE NNSA ADMINISTRATOR.

   a. Develop PCSPs that incorporate FISMA security and reporting requirements, the requirements of this Manual and comply with the requirements in DOE CIO Cyber Security Technical and Management Requirement documents as they apply to national security data and information systems within DOE, including NNSA; and ensure that the operating units implement PCSPs on National Security Systems.

   b. Determine, assess, and document program-unique threats and risks (in addition to those presented in the Departmental Cyber Security Threat Statement and Risk Assessment).

   c. Notify the Contracting Officers to incorporate the CRD into affected contracts.

2. HEADS OF DEPARTMENTAL ELEMENTS (OTHER THAN UNDER SECRETARIES, INCLUDING THE NNSA ADMINISTRATOR).

   a. Develop PCSPs that incorporate FISMA security and reporting requirements, the requirements of this Manual and comply with the requirements in DOE CIO Cyber Security Technical and Management Requirement documents as they apply to national security data and information systems within DOE, including NNSA, or are incorporated into an extension of the DOE OCIO PCSP; and ensue that the operating units implement those requirements on National Security Systems.

   b. Determine, assess, and document program-unique threats and risks (in addition to those presented in the Departmental Cyber Security Threat Statement and Risk Assessment).

   c. Notify the Contracting Officers to incorporate the CRD into affected contracts.

3. OFFICE OF THE CHIEF INFORMATION OFFICER.

   a. Review this Manual, at least annually, and update as necessary.

   b. Develop a PCSP that incorporates FISMA security and reporting requirements, the requirements of this Manual and comply with the requirements in DOE CIO Cyber Security Technical and Management Requirement documents as they apply to national security data and information systems within DOE, including NNSA; and ensure that the operating units implement the PCSPs on National Security Systems.

c. Determine, assess, and document program-unique threats and risks (in addition to those presented in the Departmental Cyber Security Threat Statement and Risk Assessment).

d. Notify the Contracting Officers to incorporate the CRD into affected contracts.

4. CONTRACTING OFFICER.

a. Once notified of contractor applicability, incorporate the CRD into affected contracts.

b. Assisting in incorporating the CRD in new contracts when notified of the applicability.

CONTRACTOR REQUIREMENTS DOCUMENT
DOE M 205.1-4, *National Security System Manual*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors whose contracts involve National Security Systems that collect, process, store, display, create, disseminate, or transmit information

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.

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 National Security Systems; compliance with the PCSP is monitored by Senior DOE Management.