Cyber Security Technical and Management Requirements

DOE Cyber Security Program Foundation (TMR-0)
August 10, 2007

The Department of Energy (DOE) governance model for managing cyber security is described in the DOE O 205.1A, *Department of Energy Cyber Security Management*, which was signed in December 2006. This Directive "establishes the high-level Departmental Cyber Security Management structure for ensuring the protection of information and information systems." Its key objectives include:

- Establishing line management accountability through Senior DOE Management (the Under Secretaries, including the National Nuclear Security Administration [NNSA] Administrator, the Administrator of the Energy Information Administration [EIA], the Administrators of the Power Marketing Administrations [PMAs], and the DOE Chief Information Officer [CIO]).
- Providing Senior DOE Management with a framework and technical and management requirements for applying cyber security controls to meet mission-specific objectives.
- Establishing a Departmental cyber security management structure that can adapt to emerging technologies and respond to the evolving threat environment.

DOE O 205.1A charges Senior DOE Management to implement cyber security within its respective organizations, based on determination, assessment, and documentation of program-unique threats and risks, as well as threats and risks identified in the Department's Cyber Security Threat Statement and Risk Assessment. In carrying out this charge, Senior DOE Management is required by this Order to develop a Program Cyber Security Plan (PCSP) that defines cyber security requirements to be implemented in all organizations under the purview of the Senior Manager. The Order also requires that the PCSPs and other organizational cyber security documentation comply with the Federal Information Security Management Act of 2002 (FISMA), Presidential Directives and Executive Orders, Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), Departmental policies, and the DOE CIO Cyber Security Technical and Management Requirements (TMRs).

The Departmental cyber security program supports strong security controls through formal policy and CIO TMRs that link policy with technical guidelines, standards, and procedures and offer approaches to implementing policy that meet organizational goals. This document establishes the "foundation" for the TMR series of documents. The TMRs support DOE implementation of OMB directives and memoranda, urgent Government-wide or DOE requirements, and NIST-developed cyber security technical guidance (issued in the NIST Special Publication [SP] 800 series), providing Departmental interpretation and simplification, as appropriate. TMRs establish implementation schedules within DOE for new or changed direction, Government

priorities, requirements, and NIST guidance reports and formalize the DOE process for issuing cyber security requirements through the PCSPs. The TMR approach eliminates the need to issue this kind of direction through ad hoc memoranda, yet it enables the Department to respond quickly and appropriately to fast-changing threat environments, other rapidly developing circumstances, or new priorities. The use of TMRs for this purpose "institutionalizes" such guidance and direction, as specified in DOE O 205.1A.

This TMR outlines foundational elements that are critical to the implementation of requirements defined in the TMR library and is to be used in developing and implementing the cyber security program via Senior DOE Management PCSPs. This document has been developed and reviewed by the Cyber Security Working Group, established by the Order and is comprised of individuals identified by each member of the DOE Cyber Security Executive Steering Committee, also established by the Order. The Cyber Security Executive Steering Committee is composed 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, one PMA Administrator, and the CIO.

Special protection of DOE National Security Systems (NSS) and information is provided through implementation of DOE M 205.1-4, *National Security Systems Manual*, signed in March 2007. The Manual complements the TMRs, which are applicable to NSS as well as unclassified systems and information.

Cancellations

None.

Implementation

In accordance with the implementation schedule of each published TMR, the Senior DOE Management is to address the Departmental requirements in its PCSP. Senior DOE Management should incorporate this TMR in PCSPs and associated direction within 90 days of the TMR issue date. Other TMRs may have a shorter timeframe for implementation, based on DOE-external direction and/or changes in the threat environment.

Requirements

TMR-0-1, Federal Information Processing Standards

FISMA requires that all US Government Agencies and contractors using or operating information systems on behalf of the Government comply with the FIPS approved by the Secretary of Commerce and issued by the National Institute of Standards and Technology. The applicable FIPS issued as of the date of this TMR are shown in Table 1. FIPS do not apply to National Security Systems (as defined in FISMA). Senior DOE Management is to document in each PCSP that all FIPS are to be followed. TMRs have

been or are being prepared to provide Departmental requirements for implementation of several FIPS and are referenced in Table 1.

Table 1. Federal Information Processing Standards

Publication Number	Publication Date	Title	TMR
FIPS 113	May 1985	Computer Data Authentication	
FIPS 140-1	January 1994	Security requirements for Cryptographic Modules	TMR-12
FIPS 140-2	May 2001 December 2002	Security requirements for Cryptographic Modules Change Notice 2 for FIPS 140-2	TMR-12, TMR-22
FIPS 180-2	August 2002 February 2004	Secure Hash Standard (SHS) Change Notice for FIPS 180-2	
FIPS 181	October 1993	Automated Password Generator	
FIPS 185	February 1994	Escrowed Encryption Standard	
FIPS 186-2	January 2000 October 2001	Digital Signature Standard (DSS) Change Notice for FIPS 186-2	
FIPS 188	September 1994	Standard Security Labels for Information Transfer	
FIPS 190	September 1994	Guideline for the Use of Advanced Authentication Technology Alternatives	
FIPS 191	November 1994	Guideline for The Analysis of Local Area Network Security	
FIPS 196	February 1997	Entity Authentication Using Public Key Cryptography	
FIPS 197	November 2001	Advanced Encryption Standard	
FIPS 198	March 2002	The Keyed-Hash Message Authentication Code (HMAC)	
FIPS 199	February 2004	Standards for Security Categorization of Federal Information and Information Systems	TMR-1, TMR-2, TMR-3
FIPS 200	March 2006	Minimum Security Requirements for Federal Information and Information Systems	TMR-1, TMR-2, TMR-3
FIPS 201-1	March 2006 June 2006	Personal Identity Verification (PIV) of Federal Employees and Contractors Change Notice 1 for FIPS 201-1	

TMR-0-2, NIST Series 800 Special Publications Addressed by DOE TMRs

Senior DOE Management is to document in its PCSP how the NIST 800 Series SPs listed in Table 2 are to be followed, consistent with Departmental direction provided in TMRs that address DOE implementation of these Special Publications. Only versions of SPs that have been officially published by NIST are to be considered in the PCSP; drafts and updates under development are to be excluded from the PCSP until publication. TMRs have been or are being prepared to provide Departmental requirements for a number of these SPs and are referenced in Table 2.

Table 2. NIST Series 800 SPs Addressed by DOE TMRs

Publication Number	Publication Date	Title	TMR
SP 800-16	April 1998	Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172)	TMR-20
SP 800-18, Revision 1	February 2006	Guide for Developing Security Plans for Federal Information Systems	TMR-2
SP 800-30	July 2002	Risk Management Guide for Information Technology Systems	TMR-3
SP 800-34	June 2002	Contingency Planning Guide for Information Technology Systems	TMR-7
SP 800-36	October 2003	Guide to Selecting Information Technology Security Products	TMR-10
SP 800-37	May 2004	Guide for the Security Certification and Accreditation of Federal Information Systems	TMR-2
SP 800-40	November 2005	Creating a Patch and Vulnerability Management Program	TMR-4
SP 800-42	October 2003	Guideline on Network Security Testing	TMR-4
SP 800-47	August 2002	Security Guide for Interconnecting Information Technology Systems	TMR-5
SP 800-48	November 2002	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices	TMR-12
SP 800-53 Revision 1	December 2006	Recommended Security Controls for Federal Information Systems	TMR-1
SP 800-59	August 2003	Guideline for Identifying an Information System as a National Security System	TMR-1
SP 800-60	June 2004	Guide for Mapping Types of Information and Information Systems to Security Categories	TMR-2
SP 800-61	January 2004	Computer Security Incident Handling Guide	TMR-9
SP 800-70	May 2005	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers	TMR-8
SP 800-88	September 2006	Guidelines for Media Sanitization Errata sheet, October 2006	TMR-10

TMR-0-3, NIST 800 Series Special Publications To Be Considered for PCSPs

Senior DOE Management is to review the guidance in the NIST 800 Series SPs listed in Table 3 to determine if and how it is to be addressed, incorporated, or referenced in the PCSP. If an SP is determined as not applicable, rationale for not addressing it should be included in the PCSP.

Table 3. NIST 800 Series SPs To Be Considered for PCSPs

Publication Number	Publication Date	Title
SP 800-13	October 1995	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-14	September 1996	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-17	February 1998	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-19	October 1999	Mobile Agent Security
SP 800-20, Revised	April 2000	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
SP 800-21-1	December 2005	Guideline for Implementing Cryptography in the Federal Government, Second Edition
SP 800-24	August 2000	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-25	October 2000	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-26	November 2001 April 2005	Security Self-Assessment Guide for Information Technology Systems Revised NIST SP 800-26 System Questionnaire with NIST SP 800-53 References and Associated Security Control Mappings
SP 800-27 Revision. A	June 2004	Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A
SP 800-28	October 2001	Guidelines on Active Content and Mobile Code
SP 800-31	November 2001	Intrusion Detection Systems (IDS)
SP 800-32	February 2001	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-33	December 2001	Underlying Technical Models for Information Technology Security
SP 800-35	October 2003	Guide to Information Technology Security Services
SP 800-41	January 2002	Guidelines on Firewalls and Firewall Policy
SP 800-43	November 2002	Systems Administration Guidance for Windows 2000 Professional
SP 800-44	September 2002	Guidelines on Securing Public Web Servers
SP 800-45	February 2007	Guidelines on Electronic Mail Security
SP 800-46	August 2002	Security for Telecommuting and Broadband Communications
SP 800-49	November 2002	Federal S/MIME V3 Client Profile
SP 800-50	October 2003	Building an Information Technology Security Awareness and Training Program

Publication Number	Publication Date	Title
SP 800-51	September 2002	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-52	June 2005	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
SP 800-55	July 2003	Security Metrics Guide for Information Technology Systems
SP 800-56A	March 2006	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-57	August 2005	Recommendation on Key Management Part 1 revised March 2007.
SP 800-58	January 2005	Security Considerations for Voice Over IP Systems
SP 800-63	April 2006	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
SP 800-64, Revision 1	June 2004	Security Considerations in the Information System Development Life Cycle
SP 800-65	January 2005	Integrating Security into the Capital Planning and Investment Control Process
SP 800-66	March 2005	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-67	May 2004	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-68	October 2005	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
SP 800-69	September 2006	Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
SP 800-72	November 2004	Guidelines on PDA Forensics
SP 800-73	March 2006	Interfaces for Personal Identity Verification Errata Sheet, April 2006
SP 800-76-1	January 2007	Biometric Data Specification for Personal Identity Verification
SP 800-77	December 2005	Guide to IPsec VPNs
SP 800-78-1	August 2007	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
SP 800-79	July 2005	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
SP 800-81	May 2006	Secure Domain Name System (DNS) Deployment Guide,
SP 800-83	November 2005	Guide to Malware Incident Prevention and Handling
SP 800-84	September 2006	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-85A	April 2006	PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)

Publication Number	Publication Date	Title
SP 800-85B	July 2006	PIV Data Model Conformance Test Guidelines
SP 800-86	August 2006	Guide to Integrating Forensic Techniques into Incident Response
SP 800-87	March 2007	Codes for the Identification of Federal and Federally-Assisted Organizations
SP 800-89	November 2006	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-90	June 2006	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Revised
SP 800-92	September 2006	Guide to Computer Security Log Management
SP 800-94	February 2007	Guide to Intrusion Detection and Prevention Systems (IDPS)
SP 800-96	September 2006	PIV Card / Reader Interoperability Guidelines
SP 800-97	February 2007	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
SP 800-98	April 2007	Guidelines for Securing Radio Frequency Identification
SP 800-100	October 2006	Information Security Handbook: A Guide for Managers

TMR-0-4, Other NIST Special Publications

The NIST 800 Series Special Publications listed in Table 4 are not expected to have general applicability in DOE. However, Senior DOE Management should consider reviewing these NIST 800 Series SPs for possible application to its programs and mission and implementation in the PCSP.

Table 4. Other NIST 800 Series SPs

Publication Number	Publication Date	Title
SP 800-12	October 1995	An Introduction to Computer Security: The NIST Handbook
SP 800-15	September 1997	Minimum Interoperability Specification for PKI Components (MISPC)
SP 800-22	May 2001	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-23	August 2000	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-29	June 2001	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
SP 800-38A	December 2001	Recommendation for Block Cipher Modes of Operation - Methods and Techniques
SP 800-38B	May 2005	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

Publication Number	Publication Date	Title
SP 800-38C	May 2004	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP 800-54	June 2007	Border Gateway Protocol Security
SP 800-101	October 2006	Guidelines on Cell Phone Forensics
SP-800-104	June 2007	A Scheme for PIV Visual Card Topography

TMR-0-5, Cyber Security Roles and Responsibilities

Senior DOE Management is responsible for defining cyber security roles and responsibilities in the PCSP for all operating units, programs, and systems within the organization. This documentation will provide the foundation for ensuring that appropriate functions and activities are included in the responsibilities of each person involved in cyber security management or implementation. Consistent definition of cyber security roles and responsibilities will also encourage the use of common training materials and reduce overall training cost. In addition, upward mobility for trained incumbents in these roles will be enhanced, and management will gain flexibility in managing cyber security activities through skill-based reassignment as appropriate. The Senior DOE Management PCSP should include the following roles:

1. Cyber Security Program Manager (CSPM)
   a. CSPM Requirements
      (1) Be an employee of United States Government.
      (2) Possess professional qualifications, including training and experience, required to administer the cyber security program functions.
      (3) Have a level of authority, in writing, commensurate with the roles and responsibilities of the position as defined in the PCSP.
   b. CSPM Responsibilities. The CSPM is the Senior DOE Management organizational official responsible for:
      (1) Serve as the Senior DOE Management primary point of contact for cyber security.
      (2) Serve as representative in the Cyber Security Working Group (CSWG).
      (3) Develop, coordinate, disseminate, and maintain the organizational PCSP and guidance on all aspects of the PCSP and the cyber security, telecommunications security, TEMPEST, and Public Key Infrastructure (PKI) programs.
      (4) Develop, disseminate, and maintain the Senior DOE Management threat descriptions, risk assessment, and approved minimum information system configuration controls.

(5) Establish and coordinate the Senior DOE Management cyber security training, education, and awareness programs.

(6) Monitor PCSP effectiveness and compliance with FISMA, Presidential directives and Executive orders, OMB directives, FIPS, Departmental policies, and DOE CIO Cyber Security TMRs.

(7) Monitor operating unit compliance with the PCSP through program reviews, budget reviews, self-assessments, management assessments, performance metrics analysis, and analysis of the results of peer reviews, vulnerability analysis, and independent oversight evaluations.

2. Designated Approving Authority (DAA). The DAA is the Senior DOE Management Federal official with the authority to formally assume responsibility and be held fully accountable for operating an information system at an acceptable level of risk. (See DOE Order 205.1A for delegation of authority.)

a. DAA Requirements

(1) Be an employee of United States Government.

(2) Have a level of authority, in writing, commensurate with accepting the risk of operating all information systems under the DAA's jurisdiction.

(3) Understand the operational need and role in mission achievement for the system(s) in question and the operational consequences of *not* operating the system(s). The DAA need not be technically trained to evaluate an information system but can be assisted by one or more DAA Representatives knowledgeable in cyber security.

b. DAA Responsibilities include:

(1) Approve the operation (accreditation or re-accreditation) of the information system, grant an Interim Approval to Operate under specific terms and conditions, or decline to accredit.

(2) Act as liaison and provide cyber security incident coordination with Law Enforcement Agencies, safeguards and security organizations, Office of Inspector General, and Office of Intelligence and Counterintelligence for the operating units under his/her cognizance.

(3) Act as liaison and provide coordination with Senior DOE Management and other operating units within the Senior DOE Management organization for all aspects of the cyber security program at the operating unit level.

(4) Complete DOE- and Senior DOE Management-sponsored DAA training within six (6) months of assuming the DAA position.

(5) Participate in an ongoing Senior DOE Management cyber security training and awareness program.

(6) Provide input to the intelligence system DAA as a result of certification and accreditation (C&A) reviews of National Security Systems that process intelligence information and Restricted Data (RD) on the adequacy of RD protection.

3. Designated Approving Authority Representative. The DAA Representative provides technical and organizational support to the DAA. The DAA Representative functions may be performed by the DAA; however, if the functions are delegated, the role should be filled by one or more technical experts responsible to the DAA for ensuring that cyber security is integrated into and implemented throughout the life cycle of a system and that the PCSP is implemented appropriately. The individual(s) in the DAA Representative role should have a working knowledge of system function, security policies, and technical security safeguards, and serve as technical advisor(s) to the DAA. The DAA Representative is to participate in an ongoing Senior DOE Management cyber security training and awareness program appropriate to assigned responsibilities.

4. Certification Agent (CA).

   a. CA Requirements

      (1) Have a working knowledge of system function, security policies, and technical security safeguards.

      (2) To ensure the integrity of the certification assessment, the certification agent should be independent of system development and operations teams as well as those individuals responsible for correcting security deficiencies identified during the assessment.

   b. CA Responsibilities

      (1) Conduct comprehensive assessment of the management, operational, assurance, and technical security controls in an information system.

      (2) Provide the System Owner with the level of effort and resource requirements for the conduct of the ST&E process.

5. Information System Security Manager (ISSM).

   a. ISSM Requirements

      (1) Have a working knowledge of system functions, cyber security policies, and technical cyber security protection measures.

      (2) Be appointed in writing by the operating unit senior manager.

   b. ISSM Responsibilities

      (1) Act as the operating unit cyber security point of contact and responsible for the operating unit's cyber security program.

(2) May serve as the CA for systems within the operating unit.

(3) Establish, document, and monitor the operating unit's cyber security program implementation and ensure operating unit compliance with the Senior DOE Management PCSP.

(4) Ensure that POA&Ms are prepared and coordinated with other security disciplines, as necessary, for program or system level findings.

(5) Ensure that the organization plans, budgets, allocates, and spends adequate resources in support of cyber security.

(6) Oversee all operating unit Information System Security Officers (ISSOs) to ensure they follow established information security policies and procedures.

(7) Ensure that a record copy of each C&A Package is maintained.

(8) Ensure that users are trained on the information system's cyber security features, operation, and safeguards prior to being allowed access to the system.

(9) Ensure that personnel with cyber security responsibilities are trained on cyber security requirements, operations, safeguards, INFOCON, and incident handling procedures.

(10) Identify and document in coordination with the operating unit's Operations Security (OPSEC) program, operating unit-specific threats to information systems and information.

(11) Ensure the operating unit cyber security program is coordinated with other operating unit plans/programs to include: disaster recovery, Site Safeguards and Security Plan or Site Security Plan, Classified Matter Protection and Control, Physical Security, Personnel Security, Telecommunications Security, TEMPEST, Technical Surveillance Countermeasures, Operations Security, Counter Intelligence, and Nuclear Materials Control and Accountability.

(12) Ensure that the cognizant DAA/DAA Representative is notified when the information system is no longer needed or when changes occur that might affect the accreditation of the information system.

(13) Participate in DOE- and Senior DOE Management-sponsored cyber security training within six (6) months of his/her appointment.

(14) Ensure a DAA-approved overwrite method is used for sanitization and a review of the results of overwrites to verify the method used completely overwrote all classified or sensitive information.

(15) Ensure CIAC alerts are analyzed, necessary corrective actions are accomplished, and the status reported and suspected cyber security incidents are investigated, analyzed, documented, and reported to the DAA/DAA Representative.

(16) Conduct self-assessments in accordance with the Senior DOE Management PCSP.

(17) Recommend changes in the operating unit INFOCON status.

(18) Ensure each individual responsible for a major application within the operating unit is aware of and fulfills his / her cyber security duties as described in the Senior DOE Management PCSP.

6. System Owner (includes Major Application Owner)/Program Manager. The System Owner is the operating unit official responsible for the overall procurement, development, integration, modification, operation, and maintenance of an information system. The System Owner responsibilities include:

   a. Coordinate all aspects of the system for which he or she is responsible from initial concept, through development, to implementation and system maintenance. The System Owner is a key contributor to the cyber security of the information system and coordinates the system design to ensure the security and user operational needs are optimized.

   b. Create and maintain POA&Ms throughout the information system's life cycle.

   c. Ensure users are authorized access to information/ data on the system prior to granting system access.

7. Information System Security Officer (ISSO). The ISSO is the individual responsible to the ISSM, information owner, and System Owner for ensuring the appropriate operational security posture is maintained for an information system. Multiple information systems may be assigned to a single ISSO. The following responsibilities apply to the ISSO.

   a. ISSO Requirements

      (1) Have a working knowledge of system functions, cyber security policies, and technical cyber security protection measures.

      (2) Has the detailed knowledge and expertise required to manage the security aspects of the information system and is generally assigned responsibility for the day-to-day security operations of the system.

      (3) Be appointed in writing.

   b. ISSO Responsibilities

      (1) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

(2) Ensure the implementation of cyber protection controls and procedures that are documented in, or referenced by, the System Security Plan for each information system for which he/she is the ISSO.

(3) Ensure that all users have the requisite security clearances, authorization, and need-to-know, and are aware of their security responsibilities before granting access to the information system.

(4) Ensure that each information system user acknowledges, in writing or electronically using DOE or Senior DOE Management-approved digital signature technologies, his/her responsibility (Code of Conduct) for the security of information systems and information.

(5) Maintain a record copy of the C&A Package for each information system for which he/she is the ISSO.

(6) Ensure that the cognizant ISSM is notified when an information system is no longer needed or when changes are planned that might affect the accreditation of the information system.

(7) Participate in the ISSM's self-assessment and training programs.

(8) Communicate individual incident and potential incident reports to the ISSM and initiate ISSM approved protective or corrective actions.

(9) Ensure that unauthorized personnel are not granted use of, or access to, the information system.

(10) Provide written notification to the cognizant information owner(s) prior to granting any foreign national access to the information system.

TMR-0-6, Senior DOE Management Deviation Processes

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing processes for granting deviations (e.g., variances, waivers, and exceptions) from the requirements of the PCSP based on mission and risk for all operating units, programs, and systems within the organization.

References

U.S. Public Laws

Federal Information Security Management Act (FISMA, enacted December 2002) - This Act (Title III of the E-Government Act of 2002) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), also known as Information Technology Management Reform Act of 1996, (Public. Law 104-106), February 1996.

E-Government Act of 2002 (Public Law 107-347), December 2002.

Office of Management and Budget (OMB)

Circular A-130, *Management of Federal Information Resources*

Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources,* Appendix III, *Security of Federal Automated Information Resources,* November 2000.

Department of Energy Directives

DOE P 205.1, Departmental Cyber Security Management Policy, dated 5-8-01.

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

DOE O 205.1A, Departmental Cyber Security Management, dated 12-4-06.

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

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

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

DOE O 470.4A, Safeguards and Security Program, dated 5-25-07.

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

DOE O 471.3, Identifying and Protecting Official Use Only Information, dated 4-9-03.

DOE O 475.1, Counterintelligence Program, dated 12-10-04.

DOE M 205.1-3, Telecommunications Security Manual, dated 4-17-06

DOE M 205.1-4, National Security System Manual, dated 3-8-07.

DOE N 142.1, Unclassified Foreign Visits and Assignments, dated 7-14-99.

DOE N 221.13, Reporting Fraud, Waste, and Abuse, dated 12-15-06.

Other

Executive Order (EO) 12344, *Naval Nuclear Propulsion Program,* dated 2-1-82.

EO 12829, *National Industrial Security Program,* dated 1-6-93.

EO 12958, *Classified National Security Information, as Amended,* dated 3-25-03.

EO 13011, *Federal Information Technology,* dated 7-16-96.

EO 13231, *Critical Infrastructure Protection in the Information Age,* dated 10-16-01.

Homeland Security Presidential Directive (HSPD)-7, *Critical Infrastructure Identification, Prioritization, and Protection,* dated 12-17-03.

HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* dated 8-27-04.

National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems,* dated 7-5-90.

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