MANUAL

DOE M 205.1-5

Approved: 8-12-08

CYBER SECURITY PROCESS REQUIREMENTS 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

CYBER SECURITY PROCESS REQUIREMENTS MANUAL

1. PURPOSE. This Department of Energy (DOE) Manual establishes the minimum requirements for cyber security management processes for national security and unclassified information throughout the Department. These requirements must be followed in the management and operation of all information systems operated by DOE and the information systems operated by contractors on behalf of the Department. This Manual is also the basis for any supplemental requirements defined by Senior DOE Management Program Cyber Security Plans (PCSPs).

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. Departmental Elements. Except for the exclusions in paragraph 3c, this Manual applies to Departmental elements that utilize Federal Information Systems (hereafter called DOE Information Systems) to collect, process, store, display, create, disseminate, or transmit national security or unclassified information, including those created after the Manual is issued. (Go to www.directives.doe.gov/pdfs/reftools/org-list.pdf for the current listing of Departmental elements).

   The Administrator of the 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 contracts that include the CRD.

      (2) The CRD must be included in contracts that involve information systems that are used or operated on behalf of DOE, including NNSA, to collect, possess, store, display, create, disseminate, or transmit national security or unclassified DOE/Government information.

      (3) 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 (e.g., contracts that involve DOE Information Systems and contain DEAR clause 952.204-2, *Security Requirements*) will be communicated as appropriate through Heads of field elements and Headquarters Departmental elements and Contracting Officers.

c. Exclusions.

(1) In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at Title 50 United States Code (U.S.C.) sections 2406 and 2511 and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval reactors (Director) will implement and oversee requirements and practices pertaining to this Manual for activities under the Director's cognizance, as deemed appropriate.

(2) Systems designated as intelligence systems are subject to the requirements of Director of National Intelligence Directives and Intelligence Community Directives and are therefore excluded from the requirements of this Manual.

4. REQUIREMENTS. This Manual establishes the minimum requirements for cyber security management processes throughout the Department. These requirements must be followed in the management and operation of all unclassified and National Security System (NSS) information systems operated by the Department.

a. A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data or other national security 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).

b. Senior DOE Management, as defined in DOE O 205.1A, Department of Energy Cyber Security Management, dated 12-4-06, can add to or strengthen these requirements for their own organizations, based on their assessment of risk, so long as any additional direction they provide to their organizations is consistent with these requirements and does not diminish the scope or effect of these DOE-wide requirements in any way.

c. Senior DOE Management PCSPs will require their operating units to implement and maintain at least the minimum requirements in this Manual for DOE information systems no more than 60 days after issuance. If an operating unit cannot implement the requirements of this Manual by the scheduled milestone, the operating unit must establish a plan of action and milestones (POA&M) for implementation of the requirements.

5. RESPONSIBILITIES. This Manual is composed of chapters that provide direction for processes, assignment of responsibilities, and supplemental requirements for protecting DOE information systems and information assets and managing cyber security processes

and is the basis for applying this direction to all Departmental elements and its contractors.

a. The Head of the Departmental element is responsible for ensuring that the CRD at Attachment 1 is included in all contracts that involve information systems used or operated by a contractor or other organization on behalf of DOE, including NNSA, to collect, process, store, display, create, disseminate, or transmit national security or unclassified DOE/Government information. Once notified, the contracting officer is responsible for incorporating the CRD into each affected contract.

b. 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.

c. The functional roles and responsibilities associated with implementing this Manual are described in Chapter I, paragraph 2 and in the CRD.

d. The Designated Approving Authority (DAA) for intelligence systems that include DOE Restricted Data is responsible for providing the certification and accreditation results to appropriate Departmental elements DAA for review.

6. REFERENCES.

a. Office of Management and Budget. Circulars are available online at http://www.whitehouse.gov/OMB/circulars/index.html.

(1) OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, Circular A-130 (11-28-00).

(2) OMB Memorandum (M) 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones (10-17-01).

(3) OMB M 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems (3-22-07).

b. Homeland Security Presidential Directives. HSPDs are available online at http://www.dhs.gov/xabout/laws/editorial_0607.shtm.

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

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

c. National Security.

(1) National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated 7-5-90 (online at http://www.fas.org/irp/offdocs/nsd/nsd_42.htm).

(2) National Security Telecommunications and Information Systems Security Committee Directive No. 500, *Information Systems Security (INFOSEC) Education, Training, and Awareness*, dated 8-2006 (online at http://stinet.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA362604).

(3) National Security Telecommunications and Information Systems Security Committee Directive No. 501, *National Training Program for Information Systems Security (INFOSEC) Professionals*, dated 11-16-92 (online at http://www.cnss.gov/Assets/pdf/nstissd_501.pdf).

(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 (online at http://www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf).

(5) National Security Telecommunications and Information System Security Instruction No. 1000, *National Information Assurance Certification and Accreditation Process*, dated April 2000 (online at http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf).

(6) National Industrial Security Program Operating Manual, dated 2-28-06 (online at http://nsi.org/Library/Govt/Nispom.html).

d. Federal Information Processing Standards. FIPS publications are available online at http://www.itl.nist.gov/fipspubs/by-num.htm.

(1) Federal Information Processing Standard (FIPS) 113, *Computer Data Authentication*, May 1985.

(2) FIPS 140-1, *Security Requirements for Cryptographic Modules*, January 1994.

(3) FIPS 140-2, *Security requirements for Cryptographic Modules*, Change Notice 2, December 2002.

(4) FIPS 180-2, *Secure Hash Standard (SHS)*, with Change Notice 1, February 2004.

(5) FIPS 181, *Automated Password Generator*, October 1993.

(6) FIPS 185, *Escrowed Encryption Standard*, February 1994.

(7) FIPS 186-2, *Digital Signature Standard (DSS)*, with Change Notice 1, October 2001.

(8) FIPS 188, *Standard Security Labels for Information Transfer*, September 1994.

(9) FIPS 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994.

(10) FIPS 191, *Guideline for The Analysis of Local Area Network Security*, November 1994.

(11) FIPS 196, *Entity Authentication Using Public Key Cryptography*, February 1997.

(12) FIPS 197, *Advanced Encryption Standard*, November 2001.

(13) FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

(14) FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

(15) FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

(16) FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Change Notice 1, June 2006.

e. National Institute of Standards and Technology. NIST publications are available online at http://csrc.nist.gov/publications/PubsSPs.html.

(1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

(2) NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

(3) NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

(4) NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

(5) NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003.

(6) NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

(7) NIST SP 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005.

(8) NIST SP 800-42, *Guideline on Network Security Testing*, October 2003.

(9) NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

(10) NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002.

(11) NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007.

(12) NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

(13) NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

(14) NIST SP 800-61, *Computer Security Incident Handling Guide*, January 2004.

(15) NIST SP 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.

(16) NIST SP 800-88, *Guidelines for Media Sanitization*, September 2006.

(17) NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

f. DOE Directives. Find directives online at www.directives.doe.gov.

(1) DOE O 142.3, Chg 1, *Unclassified Foreign Visits and Assignments Program*, dated 6-18-04.

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

(3) DOE O 205.1A, *Department Cyber Security Management*, dated 12-4-06.

(4) DOE M 205.1-3, *Telecommunications Security Manual*, dated 4-17-06.

(5) DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.

(6) DOE N 206.5, *Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information*, dated 10-9-07.

(7) DOE N 221.14, *Reporting Fraud, Waste and Abuse*, dated 12-20-07.

(8) DOE O 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 4-19-08.

(9) DOE O 221.2A, *Cooperation with the Office of Inspector General*, dated 2-25-08.

(10) DOE O 243.1, *Record Management Program*, dated 02-03-06

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

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

(13) DOE O 470.4A, *Safeguards and Security Program*, dated 5-25-07.

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

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

(16) DOE O 475.1, *Counterintelligence Program*, dated 12-10-04.

g. Other.

(1) 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.

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

(3) Title III, P.L. 107-347, Federal Information Security Management Act of 2002 (FISMA), December 2002.

(4) Title 40, Subtitle III, Information Technology Management, Also known as: Clinger-Cohen Act of 1996 (40 U.S.C. 11101), February 1996.

(5) P.L. 83-703, Atomic Energy Act of 1954 as amended by P.L. 93-438, Energy Reorganization Act of 1974.

(6) P.L. 107-347, E-Government Act of 2002, December 2002.

(7) E.O. 13010, *Critical Infrastructure Protection*, as amended, dated July 15, 1996.

(8) E.O. 13011, Federal Information Technology, dated 7-16-96.

(9) E.O. 13231, Critical Infrastructure Protection in the Information Age, dated 10-16-01.

7. DEFINITIONS.

a. Accreditation. The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

b. Certification. A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented corrected, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

c. Controlled Interface**.** A Controlled Interface (CI) provides controls to allow information flow based on its information security attributes. NOTE: The CI function may be accomplished through the use of one or more information resources of a system.

d. External Systems. External Information Systems (EIS) are information technology resources and devices that are personally owned, corporately owned, or external to an accredited system's boundary, Neither the operating unit or the accredited system owner typically does not have any direct control over the application of required security controls or the assessment of security control effectiveness of the external system.

e. Information System (IS)**.** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, transmission, disposition, or dissemination of information [SOURCE: NIST SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec.3502; OMB Circular A-130, App. III]. NOTE: Information systems include personnel, hardware, software, and procedures that support the operation of the system. An information system may be a General Support System or Major Application and include specialized systems such as industrial/process

control systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

f. Operating Unit. An Operating Unit is a subordinate element, such as a program office, field office, or contractor, reporting to an Under Secretary, the Department of Energy Chief Information Officer, the Power Marketing Administrations, or Heads of Departmental elements.

g. Security Attribute. A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes (FIPS 188). Security attributes can include: information sensitivity, need-to-know requirements, authorized senders/recipients, source and destination addresses, information domain authorizations, etc.

8. 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:

JEFFREY KUPFER
Acting Deputy Secretary

CONTENTS

CHAPTER I. FOUNDATION REQUIREMENTS

1. INTRODUCTION. This chapter defines the national security and unclassified cyber security program functional roles and responsibilities and defines a process for granting equivalencies and exceptions.

2. CYBER SECURITY FUNCTIONAL ROLES AND RESPONSIBILITIES. The cyber security program will include the following functional roles. Not all roles identified below are required for every organization; however, all functions must be accomplished. Individuals may hold multiple roles, except that the Designated Approving Authority cannot be the Certification Agent.

   a. Designated Approving Authority (DAA). The DAA is the Senior DOE Management official with the authority to formally assume responsibility and be held fully accountable for ensuring the operation of an information system at an acceptable level of risk for a particular Departmental element. The DAA authority may be delegated from Senior DOE Management in accordance with DOE O 205.1A.

      (1) The functional role of DAA must be fulfilled by an individual who—

         (a) is an employee of United States Government,

         (b) has a level of authority, in writing, commensurate with accepting the risk of operating all information systems under the DAA's jurisdiction, and

         (c) understands the operational need and role in mission achievement for the systems in question and the operational consequences of not operating the systems.

         NOTE: 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.

      (2) Responsibilities.

         (a) Approves the operation (accreditation or re-accreditation) of the information system, grants interim approval to operate under specific terms and conditions, or declines to accredit.

         (b) Provides 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.

(c) Within six (6) months of assuming the DAA position, completes DOE- and Senior DOE Management sponsored DAA training.

(d) Participates in ongoing Senior DOE Management cyber security training and awareness program.

(e) Provides input on the adequacy of Restricted Data (RD) protection to the intelligence system DAA based on a reviews of certification and accreditation (C&A) results for National Security Systems that process intelligence information and RD.

b. Cyber Security Program Manager (CSPM). Senior DOE Management will assign an individual to serve as the Cyber Security Program Manager (CSPM).

(1) The functional role of CSPM must be fulfilled by an individual who—

(a) Is an employee of United States Government;

(b) Possesses professional qualifications, including training and experience, required to administer the cyber security program functions; and

(c) Has, documented in writing, a level of authority commensurate with the responsibilities of the position.

(2) Responsibilities.

(a) Manages the cyber security program within the Senior DOE Management Organization and except for the DAA's accreditation and outside (e.g., law enforcement, etc.) incident coordination responsibilities serves as the primary point of contact for cyber security program activities.

(b) Coordinates program level aspects of the cyber security program with operating units in the Senior DOE Management organization.

(c) Acts as a liaison and coordinates the Senior DOE Management's cyber security program (e.g., policy issues, inspections, etc.) with cognizant DOE organizations.

(d) Develops, coordinates, disseminates, and maintains the organizational policy and guidance on the cyber security, telecommunications security, TEMPEST, and public key infrastructure (PKI) programs.

(e) Develops, disseminates, and maintains organizational threat descriptions, risk assessments, and approved minimum information system configuration controls.

(f) Establishes and coordinates the cyber security training, education, and awareness programs.

(g) Monitors compliance with Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, OMB memoranda, FIPS, Departmental policies, and DOE cyber security directives.

(h) Monitors compliance with policy 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.

c. DAA Representative. The DAA Representative provides technical and organizational support to the DAA. NOTE: DAA representative functions may be performed by the DAA.

(1) The functional role of DAA Representative must be fulfilled by an individual or individuals who—

(a) are appointed in writing by the DAA,

(b) have a working knowledge of system function, security policies, and technical security safeguards, and serve as technical advisors to the DAA and

(c) participate in cyber security training appropriate to assigned responsibilities.

(2) The DAA representative role is not required. The DAA can retain any or all functions that may be performed by the DAA representative; however, if the DAA delegates functions, the DAA representative role will be filled by one or more technical experts who can advise the DAA on appropriate implementation of cyber security throughout the system life.

d. Information Systems Security Manager (ISSM). The Information Systems Security Manager is the operating unit official who is responsible to the Operating Unit Manager for ensuring the implementation of the DOE cyber security program at the operating unit.

(1) The functional role of ISSM must be fulfilled by an individual who—

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

(b) is appointed in writing by the Operating Unit Manager.

(2) Responsibilities.

(a) Acts as the operating unit cyber security point of contact and is responsible for the operating unit's cyber security program.

(b) May serve as the Certification Agent (CA, see section e below) for systems within the operating unit.

(c) Establishes, documents, and monitors the operating unit's cyber security program implementation and ensures operating unit compliance with Departmental policy and the Senior DOE Management PCSP.

(d) Ensures that plan of action and milestones (POA&Ms) are prepared and coordinated with other security disciplines, as necessary, for program or system level findings.

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

(f) Oversees all operating unit information system security officers (ISSOs) to ensure that they follow established information security policies and procedures.

(g) Ensures that a record copy of each C&A package is maintained.

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

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

(j) In coordination with the operating unit's operations security (OPSEC) program, identifies and documents operating unit-specific threats to information systems and information.

(k) Ensures that 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, counterintelligence, and nuclear materials control and accountability.

(l) Ensures 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.

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

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

(o) Ensures that computer incident advisory capability alerts are analyzed, necessary corrective actions are accomplished, and status reported and that suspected cyber security incidents are investigated, analyzed, documented, and reported to the DAA/DAA representative.

(p) Ensures that self-assessments are conducted

(q) Ensures that each individual responsible for a major application within the operating unit is aware of and fulfills his/her cyber security duties.

e. Certification Agent (CA). The CA supports the ISSM. The CA provides independence in evaluating the functionality and assurance of systems developed and fielded by system owners. It is envisioned that each operating unit would be supported by a CA and depending on the organization the CA may have full time staff support or may draw part time support from within/without the operating unit.

(1) The functional role of CA must be fulfilled by an individual who—

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

(b) works independently of system development and operations teams and individuals responsible for correcting security deficiencies identified during the certification assessment to ensure the integrity of the assessment.

(c) NOTE: For moderate and high impact systems, as categorized by the C&A process in this manual, and for all protection indices, as categorized by DOE M 205.1-4, the system owner will not act as certification agent.

(2) Responsibilities.

(a) Conducts comprehensive assessment of management, operational, assurance, and technical security controls in an information system.

(b) Provides the system owner with the level of effort and resource requirements for conducting the security testing and evaluation (ST&E) process.

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

(1) Coordinates all aspects of the system for which he or she is responsible from initial concept through development to implementation, system maintenance, retirement, and disposition.

(2) Creates and maintains POA&Ms throughout the information system's life cycle.

(3) Ensures that users are authorized access to information/data on the system prior to granting system access.

g. Information System Security Officer (ISSO). The ISSO is an individual associated with an information system who responsible to the ISSM, information owner, and system owner for ensuring the appropriate cyber security posture is maintained for the information system. Multiple information systems may be assigned to a single ISSO.

(1) The functional role of ISSO must be fulfilled by an individual who—

(a) has a working knowledge of system functions, cyber security policies, and technical cyber security protection measures;

(b) 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; and

(c) is appointed in writing.

(2) Responsibilities.

(a) Ensures that each user accesses only that data, control information, software, hardware, and firmware for which he or she has authorized access and has a need-to-know and assumes only those roles and privileges for which he or she is authorized.

(b) Ensures 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.

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

(d) Ensures that each information system user acknowledges, in writing or electronically using DOE approved digital signature technologies, his/her responsibility (code of conduct) for the security of information systems and information.

(e) Maintains a record copy of the C&A package for each information system for which he/she is the ISSO.

(f) Ensures 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.

(g) Participates in ISSM self-assessment and training programs.

(h) Communicates individual incident and potential incident reports to the ISSM and initiates ISSM-approved protective or corrective actions.

(i) Ensures that unauthorized personnel are not granted use of or access to the information system.

(j) Provides written notification to the cognizant information owners prior to granting any foreign national access to the information system.

3. EQUIVALENCIES AND EXMPTIONS. Requests for equivalencies and exemptions from the requirements of this Manual must be supported with a risk assessment that identifies the risks to be accepted, compensatory measures, and alternative controls to be implemented.

a. Equivalencies. Equivalencies are approved conditions that technically differ from a requirement in this Manual but afford DAA-approved equivalent levels of protection either with or without compensatory measures.

(1) Equivalency requests must be submitted in writing to the cognizant DAA and include detailed description of the requirement(s) and rationale for the equivalency. The equivalency documentation will be included or referenced in the system security plan (SSP).

(2) The cognizant DAA will review and approve or disapprove the equivalency with comments and recommendations in writing.

(3) Equivalencies will be approved for no longer than 3 years, can be extended through request resubmission and must be documented or referenced in the SSP.

b. Exemptions. Exemptions are approved deviations from a requirement in this Manual that may create a security vulnerability. Exemptions will be approved only when correction of the condition is not feasible or cost effective and compensatory measures are inadequate to preclude the acceptance of risk.

(1) Requests for exemptions and supporting documentation must be submitted in writing by the DAA to the cognizant Senior DOE Management for review and approval. Documentation supporting the exception request and DAA's acceptance of associated residual risk must identify the requirements that cannot be met, compensatory measures implemented, and compensatory measures performance testing to validate the compensatory measures.

(2) The cognizant Senior DOE Management will review and approve or disapprove the exception request and provide a final decision in writing to the DAA. A copy of the approved exception will be provided to the DOE CIO.

(3) Approved exceptions will remain in effect no longer than 3 years and must be documented or referenced in the SSP.

CHAPTER II. CERTIFICATION AND ACCREDITATION REQUIREMENTS

1. INTRODUCTION. Federal Agencies are required by Office of Management and Budget (OMB) Circular A-130, Appendix III, to establish a process to ensure that adequate security controls are provided for all information systems. The proper implementation of a certification and accreditation (C&A) process ensures that all applicable requirements have been integrated into the development and operational processes. The C&A process implements the concept of "adequate security," or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. All systems must complete C&A prior to going operational (i.e., processing live data or information).

   a. The Certification and Accreditation (C&A) of all DOE information systems must be performed every 3 years or after any significant system changes that require that the system be re-accredited.

   b. Each DOE information system shall be accredited using one of the following forms of accreditation.

      (1) System accreditation is for a single information system operating under a single System Security Plan (SSP). Accreditation is based on information system certification.

      (2) Site accreditation is to accredit multiple instances of an information system where all identical installations (instantiations) of the information system are located at an operating unit facility(ies). Each instantiation of the information system is implemented using the same SSP. Accreditation is based on the certification of the first system and the approval of processes for testing and certifying additional instantiations. The authority to operate additional instantiations under the SSP is based on successful completion of the follow-on processes described in the SSP.

      (3) Type accreditation is to accredit multiple instances of an information system where instantiations of the information system are located at different operating unit facility(ies) but a single DAA is responsible for the system. Each instantiation of the information system has been implemented using the same SSP. Accreditation is based on the certification of the first system and approval of processes for testing and certifying additional instantiations. The authority to operate additional instantiations under the SSP is based on successful completion of the follow-on processes described in the SSP

   c. A successful C&A process provides assurance that—

      (1) the information system has adequate and effective security controls,

      (2) that system vulnerabilities have been considered and

(3) appropriate plans and funds have been identified to correct any deficiencies.

d. Assessment of an information system's security controls determines which controls are in place, implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

e. The C&A process establishes a common approach for the specific tasks and sub-tasks necessary to complete the C&A of an information system. The four major phases to the C&A methodology are—

(1) Initiation--establishing security requirements, C&A boundary, schedule, level of effort, and resources required;

(2) Certification --conducting a security assessment of controls, documenting residual risks, and producing the C&A package;

(3) Accreditation --evaluating the residual risk, making the accreditation decision, and documenting the decision as part of the C&A package; and

(4) Continuous Monitoring--ensuring the continued operation and maintenance of the system to preserve an acceptable level of residual risk.

2. C&A PROCESS. The C&A process will include the following phases and specify the required formats for documentation in each phase.

a. C&A Initiation Phase allows an organization to determine the information system security status quickly and identify changes that have to be made to attain or maintain compliance with the Federal, Departmental, and Senior DOE Management PCSP requirements.

(1) Preparation task steps will include the following.

(a) Describe the information system in the system security plan (SSP).

(b) Categorization of the information system using the process described by NIST FIPS 199 or DOE M 205.1-4, as applicable.

(c) Identify and document potential threats, vulnerabilities, and risks.

(d) Document implemented and planned security controls in the SSP.

(2) Notification and resource identification task steps will include the following.

(a) Determine the resources needed to accomplish C&A.

(b) Create a POA&M for execution and budget input and provide it to the DAA.

(c) Notify all stakeholders that C&A activities are to be accomplished.

(3) SSP analysis and acceptance task steps will include the following.

(a) Complete an independent review of the SSP, conducted or overseen by the Certification Agent and DAA. The review will include a verification that: the system security categorization is correct; the documented vulnerabilities, threats, and associated risks are accurate; and the implemented and planned controls are sufficient.

(b) Update the SSP with any findings from the independent reviews.

(c) DAA written approval of the SSP prior to progressing to the next C&A phase.

b. Certification Phase. The Certification phase demonstrates, through independent validation using specified verification techniques and procedures, the security controls for the information system have been implemented correctly and are effective in their application.

(1) Security control assessment task steps will include the following.

(a) Define ST&E procedures.

1 For a low impact unclassified system, a self-assessment can be substituted for ST&E.

2 The ST&E procedures must be approved by the DAA prior to the conduct of control assessment.

3 The controls and procedures to be used for future instantiations for site and type forms of accreditation must be included as part of the ST&E procedures.

4 If a control fails the ST&E process, the control implementation can be corrected and re-assessed.

(b) Assess security controls.

(c) Prepare an ST&E Report to include test results and recommended POA&M, if applicable.

(d) The Certification Agent will develop the Security Assessment Report.

(2) Certification documentation task steps will include the following.

(a) Certification agent recommendations to the system owner for correcting any deficiencies or reducing and/or eliminating vulnerabilities identified in the security assessment.

(b) Update the SSP and risk assessment.

(c) Update the POA&M and create any additional POA&Ms as needed.

(d) Assemble the certification and accreditation (C&A) package (see paragraph 3 below for package contents) for the DAA.

c. Accreditation Phase. The accreditation phase determines if remaining vulnerabilities pose an acceptable level of risk.

(1) Accreditation Decision.

(a) DAA determination of the residual risk.

(b) DAA determination if the residual risk is at an acceptable level, and preparation of a final accreditation decision letter. Decision options are:

1 Accreditation. The information system is authorized to operate as specified in the Certification Package.

2 Interim authority to operate (IATO). The information system is authorized to operate but has deficiencies that must be corrected.

a The deficiencies will not present any adverse impacts on the confidentiality of the information on the system.

b The DAA, certification agent, and system owner must agree on the proposed correction and time frames.

c A POA&M will be prepared for each proposed correction.

d The IATO period must not exceed 6 months.

3 Denial. The information system is not authorized to operate.

(2) Accreditation Documentation.

(a) Provide copies of the final certification package with original accreditation decision letter to the system owner.

(b) Update the certification package.

d. Continuous Monitoring Phase. The Continuous Monitoring phase provides oversight and monitoring of security controls by the System Owner on an ongoing basis.

(1) Configuration Management and Control. Determine security impact of proposed changes to the system.

(2) Security Control Monitoring. Perform periodic self-assessment of selected technical, operational, assurance, and management security.

(3) Status Report and Documentation. Tasks steps shall include the following:

(a) Update and document in the C&A package changes proposed during this phase.

(b) Update the POA&M and create additional POA&Ms, as needed.

(c) Report the status of the information system to the DAA.

3. ELEMENTS OF C&A PACKAGE. The following identifies the different documents that make up the C&A package. Except for the accreditation letter, all the documents are created during the initiation and certification phases.

a. System Security Plan.

(1) System Description.

(a) management information,

(b) system categorization,

(c) system composition (system components, accreditation boundary, form of accreditation)

(d) physical security environment,

(e) logical security environment,

(f) operational environment, and

(g) system security requirements.

(2) System Component Implementation.

(a) system component overview and

(b) system component controls.

(3) Interconnection Agreements.

b. Security Risk Assessment,

c. Privacy Impact Assessment,

d. Configuration Management Plan,

e. Contingency Plan,

f. Security Test and Evaluation Report,

g. Plan of Action and Milestones,

h. Security Assessment Report, and

i. Accreditation decision letter.

CHAPTER III. PLAN OF ACTION AND MILESTONES REQUIREMENTS

1. PLANS OF ACTION AND MILESTONES (POA&Ms) CONTENTS. All cyber security weaknesses identified for national security or unclassified information systems requiring corrective action will be incorporated into the POA&M process, whether or not a corrective action plan has been prepared. At a minimum, each POA&M will contain the fields required by the Office of Management and Budget (OMB)/DOE for quarterly reporting.

2. POA&M MANAGEMENT.

   a. POA&M activities for each operating unit/program/system must be reviewed and assessed on at least a quarterly basis.

   b. POA&Ms will be updated as needed when there are changes in roles and responsibilities; executive, legislative, technical or Departmental guidance; when vulnerabilities, risks or threats occur; and if new findings are identified in an audit, review, or self-assessment.

   c. Corrective action plans must be prepared for all POA&Ms that require more than 1 year to complete.

3. POA&M REPORTING.

   a. In accordance with the FISMA reporting requirements, Senior DOE Management will report quarterly POA&M status for all operating units, programs, and classified and unclassified information systems through the Office of the Chief Information Officer.

   b. At a minimum, POA&M reporting will include—

      (1) program and system-level findings for all classified and unclassified systems, including those identified by the Office of Health, Safety, and Security; General Accounting Office (GAO); and Office of Inspector General (IG);

      (2) any weaknesses and open action items resulting from internal program and system reviews;

      (3) Type 1 incidents; and

      (4) lack of self-assessments, risk assessments, security plans, privacy impact assessments, certification and accreditation, contingency plans, and implementation of PCSP and other cyber security-related requirements (e.g., requirements in program-specific Directives or contract documents).

c. Senior DOE Management will verify and validate all quarterly reports from operating units that contain no POA&Ms (i.e., no findings from any source to report).

d. Once a POA&M has been reported.

(1) Reported closure of milestones and/or findings must be validated. by someone other than the person(s) directly responsible for the closure.

(2) Closed, verified milestones will remain on the report until the finding is closed.

(3) All closed, verified findings will remain on the report for 1 year.

4. POA&M CONTENTS. All cyber security weaknesses requiring corrective action are to be incorporated into the POA&M process, whether or not a corrective action plan has been prepared. Each POA&M must contain as a minimum:

a. A brief overview and summary of the identified weakness (i.e., vulnerability, finding, etc.), written at an unclassified level.

b. Office or organization responsible for remediation.

c. Identification of program or system level issue.

d. Proposed/approved source and amount of resources required, where applicable, for remediation (i.e., funding, personnel, expertise, new system, etc.).

e. For system-level POA&Ms, the unique project identifier and project name from the OMB Exhibit 300 or Exhibit 53, where applicable. For Exhibit 53 systems, security costs must also be included.

f. Citation of source of identification of the weakness.

g. Scheduled completion date.

h. At least one major milestone and scheduled completion date.

i. Verification and documentation for the closure of each milestone.

CONTRACTOR REQUIREMENTS DOCUMENT
DOE M 205.1-5, *CYBER SECURITY PROCESS REQUIREMENTS MANUAL*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors whose contracts involve information systems that collect, process, store, display, create, disseminate, or transmit national security or unclassified DOE/Government information.

Regardless of the performer of the work, the contractor is responsible for implementing and complying with the requirements of this CRD and the applicable Senior DOE Management Program Cyber Security Plan (PCSP).

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.

Contractor managers or system owners may specify and implement additional requirements to address specific risks, vulnerabilities, or threats within its operating unit/systems.