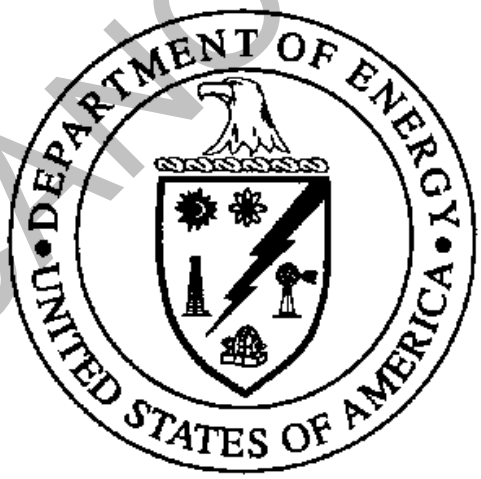
MANUAL

DOE M 205.1-7

Approved: 1-5-09
Admin Chg 1: 9-1-09

SECURITY CONTROLS FOR UNCLASSIFIED INFORMATION SYSTEMS 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

SECURITY CONTROLS FOR UNCLASSIFIED INFORMATION SYSTEMS MANUAL

1. PURPOSE. This Department of Energy (DOE) Manual establishes the minimum implementation requirements for cyber security technical, management, and operational controls that will be followed in 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 (PCSPs).

   This Manual defines for DOE, including NNSA, mandatory minimum management, operational, and technical controls for all unclassified information systems. The DOE criteria for these security controls are based on the recommendations of National Institute for Standards and Technology (NIST) Special Publication (SP) 800 53, Revision 1. This Manual is composed of two chapters that provide direction 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.

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. All Departmental Elements. Except for the exclusions in paragraph 3c, this Manual applies to Departmental elements that utilize information systems that are used or operated by DOE or a contractor or other organization on behalf of DOE, including NNSA, hereafter called DOE information systems, to collect, process, store, display, create, disseminate, or transmit 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 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. 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.

      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.

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**.**. 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.

Information systems designated as intelligence systems are subject to the requirements of the 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 implementation requirements for cyber security controls for all unclassified information systems operated by or on behalf of DOE. These requirements will be followed in the management and operation of all information systems operated by and on behalf of DOE.

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 Managers, as defined in DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06, can add to or modify 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, except for any exemptions as documented in the program cyber security plans (PCSPs).

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 later than 1-1-2010. If an operating unit cannot implement the requirements of this Manual by the scheduled milestone, the operating unit will establish a plan of action and milestones (POA&Ms) for implementation of the requirements.

Vertical line denotes change.

d. Existing accredited DOE information systems will 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. Information systems beginning the Initiation Phase of the Certification and Accreditation (C&A) process, after implementation of this Manual must accomplish accreditation in accordance with this Manual.

5. RESPONSIBILITIES.

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

6. REFERENCES.

a. Executive Orders.

(1) E.O. 13010, *Critical Infrastructure Protection*, as amended, dated7-15-96.

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

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

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. 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) o*f Federal Employees and Contractors*, Change Notice 1, June 2006.

d. 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 1, 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.

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

(1) OMB Circular A-130, Management of Federal Information Resources.

(2) OMB Transmittal Memorandum #4, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 2000.

(3) OMB M 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, dated October 17, 2001

(4) OMB M 06-16, Protection of Sensitive Agency Information, dated June 23, 2006

(5) OMB M 07-16, Safeguarding against and responding to the Breach of PII, dated May 22,2007

(6) OMB M 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems, dated March, 22, 2007

(7) OMB M-08-22, Guidance on the Federal Desktop Core Configuration (FDCC), dated August 11, 2008

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

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

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

(3) DOE O 142.3 Change 1, Unclassified Foreign Visits and Assignments, dated 6-18-04.

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

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

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

(7) DOE O 243.1, *Records Management Program*. dated 2-3-06.

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

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

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

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

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

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

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

(15) DOE M 470.4-2, *Physical Protection*, dated 8-26-05, Change 1, dated 3-7-06.

(16) DOE M 470.4-4, *Information Security*, dated 8-26-05, Change 1, dated 6-29-07.

(17) DOE N 142.3, *Unclassified Foreign Visits and Assignments*, dated 6-18-04.

(18) DOE N 206.4, *Personal Identity Verification*, dated 6-29-07.

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

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

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 (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.

(4) Clinger-Cohen Act of 1996, P.L 104-106, Divisions D and E, 110 Stat. 186 (codified as amended in scattered sections of 40 and 41 U.S.C.).

(5) Please change the reference in (6) to read as follows: Atomic Energy Act of 1954, as amended (codified at 42 U.S.C. §§ 2011-2286i, 2297f-2297g-4).

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

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

(8) National Industrial Security Program Operating Manual, dated February 28, 2006.

7. DEFINITIONS.

a. 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

b. 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.

c. 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

d. Managed/ Controlled Interface: A Managed/ 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

e. 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

f. System Administrator: Those users with "super-user", "root", or equivalent access to a system or system component; with complete control of the operating system of an information system or information system component; with permissions to set up or administer user accounts, authenticators, and the like; with permissions to change control parameters on routers, multiplexors, and other key information system equipment; or with permissions to control and change all users' access to data or program files; or with access permissions for troubleshooting information system/ security monitoring functions with specialized equipment.

g. Peer-to-Peer (P2P) Network: A peer-to-peer computer network is a network that relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. Each computer has the same capabilities and either party can initiate a communication session.

h. Privileged User: Those with limited control of the operating system of an information system or information system component such as workstations, servers, routers, multiplexors, and other key information system equipment or with access permissions for troubleshooting information system/ security monitoring functions with specialized equipment.

8. NECESSITY FINDINGS STATEMENT. In compliance with the statutory requirements in P.L. 104-201, Sec. 3174, DOE hereby finds that the subject Order is necessary for the protection of human health and the environment or safety and fulfillment of current legal requirements.

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:

JEFFREY F. KUPFER
Acting Deputy Secretary

CONTENTS

CHAPTER I. REQUIREMENTS

1. INTRODUCTION.

   a. These requirements for management, operations, and technical controls will be implemented on all DOE and NNSA unclassified information systems.

   b. The baselines defined in Tables 2 through 19 must be applied to all unclassified information systems. The baselines establish the minimum sets of controls for all DOE information systems processing unclassified information.

   c. DOE Senior Management, as defined in DOE O 205.1A, Operating Unit Managers, and System Owners may add to or modify these requirements and those identified in the PCSP, for their systems, 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, effect, or impact level of these DOE-wide requirements, except for any exemptions as documented in the PCSP .

2. EQUIVALENCIES AND EXEMPTIONS. 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.

   c. 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.

d. 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.

e. Approved exemptions will remain in effect no longer than 3 years and must be documented or referenced in the SSP.

3. SYSTEM SECURITY PLANS.

a. Each unclassified information system will be covered by a system security plan (SSP).

b. The technical, operational, and management controls that comprise the minimum set of security controls for the system will 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 will also be included in the SSP.

c. The SSP will address how the system implements the minimum technical, operational and management requirements identified in this Manual. If the impact from the loss of 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 will describe the implementation of any additional controls.

d. Security controls adopted throughout a Senior DOE Management cyber security program or within an 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 management (e.g., the same configuration management process used for multiple systems). These controls are referred to as common security controls and may be implemented by a system or multiple systems and managed under different SSPs.

(1) Common security controls will 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.

(2) Use of the controls in other information systems requires DAA-approved testing to validate correct implementation of the controls in the new information system.

(3) Other SSPs may reference the SSP of the accredited system for implementation documentation and certification test results.

4. MANAGING ORGANIZATIONAL RISK. The Senior DOE Management must document its approach to managing organizational risk in the PCSP.

a. Senior DOE Management can utilize the Equivalencies and Exemptions process to grant Exemptions to any of the requirements in this Manual. Any approved Exemptions must be documented in the PCSP in order to establish appropriate risk-based implementation direction for all Operating Units under their purview.

b. Operating Units must use the risk-based approach outlined in 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.

c. Since the potential impact values determined through use of Federal Information Processing Standard (FIPS) 199 for confidentiality, integrity, and availability may not be identical for an information system, the high-water mark concept is to be used to determine the impact level of the information system and select an initial set of security controls.

CHAPTER II. MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS

1. CYBER SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS.

This Manual utilizes the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 1, structure utilizing the control classes, families, and identifiers. This Manual also includes one additional control family,E-SU, that are DOE-specific. All control families are included in Table 1. All control families are included in Table 1.

This chapter includes tables of all NIST SP 800-53, Revision 1, controls by family and tables of additional DOE-specific controls in one family.

- If a security control is to be applied to a system and implementation documented in the SSP, the family identifier and control number are listed.
- If a control is not used, the cell is marked "not selected."[1] Control enhancements to be applied to a system and implementation documented in the SSP, are indicated parenthetically. Shaded cells in the tables indicate where controls have been modified for Departmental use. DOE changes to a NIST-derived control are in **bold font**.

a. The security control structure consists of following three key components:

(1) Control section. The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of assignment and selection operations within the main body of the control. Assignment and selection operations provide an opportunity for an organization to tailor the security controls to support specific mission, business, or operational needs.

(2) Control supplemental guidance section. The supplemental guidance section provides important additional information related to a specific security control. Organizations are expected to apply the supplemental guidance when defining, developing, and implementing security controls. In certain instances, the supplemental guidance provides more detail concerning the control requirements or important considerations

[1] The controls marked as "Not Selected" are also marked as "Not Selected" in NIST 800-53.

(and the needed flexibility) for implementing security controls in the context of an organization's operational environment, specific mission requirements, or assessment of risk.

(3) Control enhancements section. The control enhancements section provides statements of security capability to:

- build in additional, but related, functionality to a basic control; and/or
- increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment.

b. The statements of controls from NIST SP 800-53, Revision 1, have been included to provide a single document containing all technical, operational, and management controls, including the required controls for all DOE unclassified information systems.

Table 1. Cyber Security Control Classes, Families and Identifiers

CLASS	FAMILY	IDENTIFIER
Technical	Access Control	AC
Operational	Awareness and Training	AT
Technical	Audit and Accountability	AU
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Configuration Management	CM
Operational	Contingency Planning	CP
Technical	Identification and Authentication	IA
Operational	Incident Response	IR
Operational	Maintenance	MA
Operational	Media Protection	MP
Operational	Physical and Environmental Protection	PE
Management	Planning	PL
Operational	Personnel Security	PS
Management	Risk Assessment	RA
Management	System and Services Acquisition	SA
Technical	System and Communications Protection	SC
Operational	System and Information Integrity	SI
Management	Sensitive Unclassified Information	E - SU

2. **ACCESS CONTROLS**. Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. They include controls that restrict users to authorized transactions and functions and controls that limit network access and public accesses to the system.

Table 2. Access Controls

Access Controls				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3)(4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	AC-4 (6)	AC-4 (4)(5)(6)	AC-4 (4)(5)(6)
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	AC-6 (1)	AC-6 (1)	AC-6 (1)
AC-7	Unsuccessful Login Attempts	AC-7	AC-7 (1)	AC-7 (1)
AC-8	System Use Notification	AC-8 (1)	AC-8 (1)	AC-8 (1)
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12(2)	AC-12 (1)(2)
AC-13	Supervision and Review—Access Control	AC-13	AC-13(1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17 (1)(2)(3)(4) (5)(6)	AC-17 (1)(2)(3)(4) (5)(6)(7)	AC-17 (1)(2)(3)(4) (5)(6)(7)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)(2)	AC-18 (1)(2)

Access Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
AC-19	Access Control for Portable and Mobile Devices	AC-19 (1)(2)	AC-19 (1)(2)	AC-19 (1)(2)
AC-20	Use of External Information Systems	AC-20	AC-20 (1)(2)(3)	AC-20 (1)(2)(3)

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
AC-1	AC-1	AC-1

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: Account management includes—

- the identification of account types (i.e., individual, group, and system),
- establishment of conditions for group membership, and
- assignment of associated authorizations.

The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on:

- a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria and
- intended system usage.

The organization requires proper identification for requests to establish information system accounts and approves all such requests.

The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured.

Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

Control Enhancements:

(1) The organization employs automated mechanisms to support the management of information system accounts.

(2) The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

(3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

(4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

Low	Moderate	High
AC-2	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3)(4)

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are

employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is compliant with Federal Information Processing Standard (FIPS) 140-2 (as amended).

Related Security Control: SC-13.

Control Enhancements:

(1) The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Low	Moderate	High
AC-3	AC-3 (1)	AC-3 (1)

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information.

A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are:

- keeping export controlled information from being transmitted in the clear to the Internet,
- blocking outside traffic that claims to be from within the organization, and
- not passing any web requests to the Internet that is not from the internal web proxy.

Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems.

Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

Related Security Control: SC-7.

Control Enhancements:

(1) The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.

Enhancement Supplemental Guidance: Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information.

(2) The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.

(3) The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.

(4) **A managed/ controlled interface is used to adjudicate security policy and practices between interconnected systems with differing security category impact levels**

(5) **Protocols specific to peer-to-peer (P2P) server-client applications are not passed between systems or on the network unless specifically authorized in the Interconnection Security Agreement for each system hosting a P2P server-client application.**

(6) **Boundary protection services detect and block unauthorized P2P applications, services, and software ports.**

Low	Moderate	High
AC-4 (6)	AC-4 (4)(5)(6)	AC-4 (4)(5)(6)

AC-5 SEPARATION OF DUTIES

Control: The information system enforces separation of duties through assigned access authorizations.

Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include:

- mission functions and distinct information system support functions are divided among different individuals/roles;
- different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and
- security personnel who administer access control functions do not administer audit functions.

Control Enhancements: None.

Low	Moderate	High
Not Selected	AC-5	AC-5

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Control Enhancements:

(1) **The specific ports authorized for use by peer-to-peer applications are minimized.**

Low	Moderate	High
AC-6 (1)	AC-6 (1)	AC-6 (1)

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system enforces a limit of [*Assignment: **number, as specified in the information system SSP***] consecutive invalid access attempts by a user during [*Assignment: **time period, as specified in the information system SSP***]. The information system automatically [*Selection: locks the account/node for an* [*Assignment: **time period, as specified in the information system SSP**], delays next login prompt according to* [*Assignment: **delay algorithm, as specified in the information system SSP***.] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Control Enhancements:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Low	Moderate	High
AC-7	AC-7 (1)	AC-7 (1)

AC-8 SYSTEM USE NOTIFICATION

Control: The information system displays an approved, system use notification message before granting system access informing potential users:

- that the user is accessing a U.S. Government information system;
- that system usage may be monitored, recorded, and subject to audit;
- that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

- that use of the system indicates consent to monitoring and recording.

- The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Supplemental Guidance: Privacy and security policies are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

- the system use information is available and, when appropriate, is displayed before granting access;

- any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and

- the notice given to public users of the information system includes a description of the authorized uses of the system.

Control Enhancements:

(1) **The information system will display the following warning banner (or close approximation) at login and require users to electronically acknowledge the warning (such as clicking on "OK" or "I agree" button to proceed):**

****WARNING**WARNING**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.

****WARNING**WARNING**WARNING**WARNING****

Low	Moderate	High
AC-8 (1)	AC-8 (1)	AC-8 (1)

AC-9 PREVIOUS LOGON NOTIFICATION

Control: Upon successful logon, the information system notifies the user of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	Not Selected

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for any user [*Assignment:* ***number of sessions, as defined in the information system SSP***].

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	AC-10

AC-11 SESSION LOCK

Control: The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.

Control Enhancements: None.

Low	Moderate	High
Not Selected	AC-11	AC-11

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a remote session after [*Assignment:* ***time period specified in the information system SSP of no greater than 30 minutes***].

Supplemental Guidance: A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Control Enhancements:

(1) Automatic session termination applies to local and remote sessions.

(2) **Re-authentication of remote users after inactivity timeout is required**.

Low	Moderate	High
Not Selected	AC-12 (2)	AC-12 (1)(2)

AC-13 SUPERVISION AND REVIEW—ACCESS CONTROL

Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities.

The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST SP 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the review of user activities.

Low	Moderate	High
AC-13	AC-13(1)	AC-13 (1)

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov).

Related Security Control: IA-2.

Control Enhancements:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

Low	Moderate	High
AC-14	AC-14 (1)	AC-14 (1)

AC-15 AUTOMATED MARKING

Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Supplemental Guidance: Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in AC-16.

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	AC-15

AC-16 AUTOMATED LABELING

Control: The information system appropriately labels information in storage, in process, and in transmission.

Supplemental Guidance: Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with:

- access control requirements;
- special dissemination, handling, or distribution instructions; or
- as otherwise required to enforce information system security policy.

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	Not Selected

AC-17 REMOTE ACCESS

Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.

Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating **from outside the accreditation boundary.**

Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access.

The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology).

NIST SP 800-63 provides guidance on remote electronic authentication. If the Federal personal identity verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SPs 800-73 and 800-78. **DOE N 206.4, *Personal Identity Verification*, also contains DOE requirements related to authorization credentials and their issuance.**

NIST SP 800-77 provides guidance on IPsec-based virtual private networks.

Related Security Control: IA-2.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

(3) The organization controls all remote accesses through a limited number of managed access control points.

(4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

(5) **Remote access is initially granted and annually revalidated, by the user's supervisor or manager, based on authorized business needs, including scientific and other collaborative activities.**

(6) **Privileged users and administrators using remote access utilize multi-factor authentication and a trusted path capability (e.g., Virtual Private Network (VPN), Protected Transmission System (PTS), transmission medium and connection points under DOE physical control, etc.) for initial sign-on/logon.**

(7) **Systems allowing remote access use two-factor authentication and a trusted path (e.g., VPN, PTS, transmission medium and connection points under DOE physical control, etc.) for general user remote access initial sign-on/logon.**

Low	Moderate	High
AC-17 (1)(2)(3)(4)(5)(6)	AC-17 (1)(2)(3)(4)(5)(6)(7)	AC-17 (1)(2)(3)(4)(5)(6)(7)

AC-18 WIRELESS ACCESS RESTRICTIONS

***Control*:** The organization:

- establishes usage restrictions and implementation guidance for wireless technologies and
- authorizes, monitors, controls wireless access to the information system**, including:**
  - **Identification of conditions and definition of policies for introducing wireless portable/mobile systems into areas where**

sensitive unclassified and classified information is being processed.

- **Assessment of the risks to the confidentiality, integrity, and availability of operating unit information resources in the context of wireless networking devices to include the entire spatial volume of transmitted/received signal capability.**
- **Roles, responsibilities, and training of all key personnel responsible for approval, implementation, oversight, and use of wireless networks or devices.**
- **Controls used to reduce/eliminate the DOE TEMPEST/Technical Security Countermeasures (TSCM) concerns (e.g., wireless, audio, video, infrared, etc.) when allowing the operation of wireless devices in security areas.**
- **Controls used to ensure that interconnection of wireless portable/mobile systems is made only to an information system that is accredited for the interconnection.**

Supplemental Guidance: NIST SPs 800-48 and 800-97 provide guidance on wireless network security. NIST SP 800-94 provides guidance on wireless intrusion detection and prevention.

Control Enhancements:

(1) The organization uses authentication and encryption to protect wireless access to the information system.

(2) The organization scans for unauthorized wireless access points [Assignment: organization-defined frequency] and takes appropriate action if such an access points are discovered.

Enhancement Supplemental Guidance: An organization conducts a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.

Low	Moderate	High
AC-18	AC-18 (1)(2)	AC-18 (1)(2)

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Control: The organization:

- establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices and

- authorizes, monitors, and controls device access to organizational information systems.

Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include

- device identification and authentication,
- implementation of mandatory protective software (e.g., malicious code detection, firewall),
- configuration management,
- scanning devices for malicious code,
- updating virus protection software,
- scanning for critical software updates and patches,
- conducting primary operating system (and possibly other resident software) integrity checks, and
- disabling unnecessary hardware (e.g., wireless, infrared).

Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family.

Related Security Controls: MP-4, MP-5.

Control Enhancements:

(1) **Portable/mobile devices used to process SUI or in any area where SUI is processed and taken outside the United States, other than the assigned user's primary work location are subjected to a hardware and/or software technical review process upon return to detect unauthorized software, firmware, or hardware changes.**

(2) **All portable/mobile devices that process, display, store, or transmit SUI apply administrative and/or physical controls to reduce/eliminate TSCM concerns when operated in security areas.**

Low	Moderate	High
AC-19 (1)(2)	AC-19(1)(2)	AC-19(1)(2)

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions for authorized individuals to:

- access the information system from an external information system and
- process, store, and/or transmit organization-controlled information using an external information system.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to—

- personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants);
- privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports);
- information systems owned or controlled by nonfederal governmental organizations; and
- federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system.

This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems).

The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum:

- the types of applications that can be accessed on the organizational information system from the external information system and
- the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Control Enhancements:

(1) The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:

- can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan or
- has approved information system connection or processing agreements with the organizational entity hosting the external information system.

(2) **The organization has identified specific operational environments, and associated policies, within which the use of External Information Systems will be permitted and the process to determine the network boundaries of these systems.**

(3) The organization governs the use and disposition of External Information Systems that have been or are being used to access, collect, create, process, transmit, disseminate, or store sensitive unclassified information.

Low	Moderate	High
AC-20	AC-20 (1)(2)(3)	AC-20 (1)(2)(3)

3. **AWARENESS AND TRAINING CONTROLS**. Cyber security awareness consists of reminders that focus the user's attention on the concept of cyber security in the user's daily routine. Awareness provides a general cognizance or mindfulness of one's actions, and the consequences of those actions. Cyber security training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge, producing relevant and necessary security skills and competencies in those who access or manage DOE, including NNSA, information and resources.

Table 3. Awareness and Training Controls

Awareness and Training				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contact with Security Groups and Associations	Not Selected	Not Selected	Not Selected

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and

- formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SPs 800-16 and 800-50 provide guidance on security awareness and training. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
AT-1	AT-1	AT-1

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) **within 5 work days of starting in their formal capacity and** before authorizing access

to the system, when required by system changes, and [*Assignment: organization-defined frequency, **at least annually***] thereafter. **The content of organizational security awareness training will incorporate security awareness training competencies provided by the DOE CIO.**

Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in Title 5 Code of Federal Regulations (CFR) 930.301, the guidance in NIST SP 800-50, **and incorporates the requirements of the DOE CIO cyber security awareness and training program.**

Control Enhancements: None.

Low	Moderate	High
AT-2	AT-2	AT-2

AT-3 SECURITY TRAINING

Control: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training:

- before authorizing access to the system or performing assigned duties,
- when required by system changes, and
- [*Assignment: organization-defined frequency, **at least every 2 years***] thereafter.

The content of all required role-based training courses and modules will incorporate role based training competencies provided by the DOE CIO.

Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in 5 CFR930.301, the guidance in NIST SP 800-50, **and incorporates the requirements of the DOE CIO cyber security awareness and training program**.

Control Enhancements: None.

Low	Moderate	High
AT-3	AT-3	AT-3

AT-4 SECURITY TRAINING RECORDS

Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
AT-4	AT-4	AT-4

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	Not Selected

4. **AUDIT AND ACCOUNTABILITY CONTROLS**. Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can support individual accountability, a means to reconstruct events, detect intrusions, and identify problems. System audit trails, or event logs, provide a record of events in support of activities to monitor and enforce the information system security policy. NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, Chapter 18, describes an event as any action that happens on a computer system, such as logging into a system, executing a program, or opening a file.

Table 4. Audit and Accountability Controls

Audit and Accountability				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (2)(3)	AU-2 (1)(2)(3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1)(2)
AU-6	Audit Monitoring, Analysis, and Reporting	AU-6	AU-6 (2)	AU-6 (1)(2)
AU-7	Audit Reduction and Report Generation	AU-7	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Retention	AU-11	AU-11	AU-11

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and

- formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
AU-1	AU-1	AU-1

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment:* ***auditable events as described in the information system SSP***].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system.

The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function.

The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST SP 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

Low	Moderate	High
AU-2	AU-2 (2)(3)	AU-2 (1)(2)(3)

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Supplemental Guidance: Audit record content includes, for most audit records:

- date and time of the event,
- the component of the information system (e.g., software component, hardware component) where the event occurred,
- type of event,
- user/subject identity, and
- the outcome (success or failure) of the event. NIST SP 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

Low	Moderate	High
AU-3	AU-3 (1)	AU-3 (1)(2)

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements.

Related Security Controls: AU-2, AU-5, AU-6, AU-7, SI-4.

Control Enhancements: None.

Low	Moderate	High
AU-4	AU-4	AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Related Security Control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: **the percentage of maximum audit record storage capacity, as specified in the information system SSP***].

(2) The information system provides a real-time alert when the audit failure events occur: [*Assignment: audit failure events requiring real-time alerts, as specified in the information system SSP*].

Low	Moderate	High
AU-5	AU-5	AU-5 (1)(2)

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: **list of inappropriate or unusual activities that are to result in alerts as specified in the information system SSP***].

Low	Moderate	High
AU-6	AU-6 (2)	AU-6 (1)(2)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

Low	Moderate	High
AU-7	AU-7 (1)	AU-7 (1)

AU-8 TIME STAMPS

Control: The information system provides time stamps for use in audit record generation.

Supplemental Guidance: Time stamps (including date and time) of audit records are generated using internal system clocks.

Control Enhancements:

(1) The organization synchronizes internal information system clocks [*Assignment: organization-defined frequency*].

Low	Moderate	High
AU-8	AU-8 (1)	AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Control Enhancements:

(1) The information system produces audit records on hardware-enforced, write-once media.

Low	Moderate	High
AU-9	AU-9	AU-9

AU-10 NON-REPUDIATION

Control: The information system provides the capability to determine whether a given individual took a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message,

or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	Not Selected

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for [*Assignment: **a time period defined in the information system SSP and consistent with Departmental retention periods***] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST SP 800-61 provides guidance on computer security incident handling and audit record retention.

Control Enhancements: None.

Low	Moderate	High
AU-11	AU-11	AU-11

5. **CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS CONTROLS**. Certification and Accreditation (C&A) is the process of formal assessment, testing (certification), and acceptance (accreditation) of system security controls that protect information systems and data stored in and processed by those systems. It is a process that encompasses the system's life cycle and ensures that the risk of operating a system is recognized, evaluated, and accepted. 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, which is defined in OMB Circular A-130.

Table 5. Certification, Accreditation, and Security Assessments Controls

Certification, Accreditation, and Security Assessments				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1 (1)	CA-1 (1)	CA-1 (1)
CA-2	Security Assessments	CA-2	CA-2	CA-2
CA-3	Information System Connections	CA-3 (1)	CA-3 (1)	CA-3 (1)
CA-4	Security Certification	CA-4 (1)(2)	CA-4 (1)(2)	CA-4 (1)(2)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6 (1)(2)	CA-6 (1)(2)	CA-6 (1)(2)
CA-7	Continuous Monitoring	CA-7 (2)	CA-7 (2)	CA-7 (1)(2)

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

Supplemental Guidance: The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST SP 800-53A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements:

(1) **Each information system is accredited using one of the following forms of accreditation.**

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

- **Site accreditation is used to accredit multiple instances of an information system where all identical installations (instantiations) of the information system are located at an operating unit facilities. 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.**

- **Type accreditation is used to accredit multiple instances of an information system where instantiations of the information system are located at different operating unit facility(ies). 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.**

Low	Moderate	High
CA-1 (1)	CA-1 (1)	CA-1 (1)

CA-2 SECURITY ASSESSMENTS

Control: The organization conducts an assessment of all the security controls in the information system [*Assignment: organization-defined frequency, at least annually*] 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.

Supplemental Guidance: This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can

draw upon the security control assessment results from any of the following sources, including but not limited to:

- security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4),
- continuous monitoring activities (see CA-7), or
- testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness).

Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations will annually assess a subset of the security controls based on:

- the FIPS 199 security categorization of the information system,
- the specific security controls selected and employed by the organization to protect the information system, and
- the level of assurance (or confidence) that the organization will have in determining the effectiveness of the security controls in the information system.

It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST SP 800-53A provides guidance on security control assessments to include reuse of existing assessment results.

Related Security Controls: CA-4, CA-6, CA-7, SA-11.

Control Enhancements: None.

Low	Moderate	High
CA-2	CA-2	CA-2

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

Supplemental Guidance: Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST SP 800-47 provides guidance on connecting information systems.

Related Security Controls: SC-7, SA-9.

Control Enhancements:

(1) **All agreements and authorizations related to interconnected systems (i.e., Memoranda of Understanding and Interconnection Security Agreements) are documented in the SSP.**

***Enhancement Supplemental Guidance*: The MOU details the management agreement and describes responsibilities between organizations with interconnected information systems. The ISA specifies the technical security implementation of the interconnections between two systems.**

Low	Moderate	High
CA-3 (1)	CA-3 (1)	CA-3 (1)

CA-4 SECURITY CERTIFICATION

Control: The organization conducts an assessment of **all** the security controls in the information system 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.

- **Under a "system" form of accreditation, each control is subjected to an assessment (security test and evaluation) process.**
- **Under a "site or type" form of accreditation, each control of the first installation (i.e., instantiation) of a system is subjected to an assessment process, and accreditation of additional instantiation (identical installation) is based on a subset of the assessment procedures used for the first instantiation.**

Supplemental Guidance: A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST SP 800-53A provides guidance on security control assessments. NIST SP 800-37 provides guidance on security certification and accreditation.

Related Security Controls: CA-2, CA-6, SA-11.

Control Enhancements:

(1) The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.

Enhancement Supplemental Guidance: An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness.

Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization.

Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system.

The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals.

The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment of the security controls be

accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results.

The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

(2) **Assessment procedures are approved by the DAA prior to the beginning of the assessment process.**

Low	Moderate	High
CA-4 (1)(2)	CA-4 (1)(2)	CA-4 (1)(2)

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization develops and updates [*Assignment: organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Supplemental Guidance: The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, **Federal Desktop Core Configuration compliance assessments**, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems. NIST SP 800-30 provides guidance on risk mitigation.

Control Enhancements: None.

Low	Moderate	High
CA-5	CA-5	CA-5

CA-6 SECURITY ACCREDITATION

Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency, at least every three years*] or when there is a significant change to the system **or its logical, physical, or operational environment**..

Supplemental Guidance: OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three-year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST SP 800-37 provides guidance on the security certification and accreditation of information systems.

Related Security Controls: CA-2, CA-4, CA-7.

Control Enhancements:

(1) **Each general support system (GSS) or major application (MA) is accredited or have interim approval to operate (IATO) from the designated approving authority (DAA) before any DOE/Government information is processed, created, transmitted, etc. on the system.**

(2) **The DAA withdraws accreditation based on determination that the risk to the information is no longer acceptable.**

Low	Moderate	High
CA-6 (1)(2)	CA-6 (1)(2)	CA-6 (1)(2)

CA-7 CONTINUOUS MONITORING

Control: The organization monitors the security controls in the information system on an ongoing basis.

Supplemental Guidance: Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on:

- the FIPS 199 security categorization of the information system,
- the specific security controls selected and employed by the organization to protect the information system, and
- the level of assurance (or grounds for confidence) that the organization will have in determining the effectiveness of the security controls in the information system.

The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2).

This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST SP 800-37 provides guidance on the continuous monitoring process. NIST SP 800-53A provides guidance on the assessment of security controls.

Related Security Controls: CA-2, CA-4, CA-5, CA-6, CM-4.

Control Enhancements:

(1) The organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.

(2) **The organization employs a Security Content Automation Protocol (SCAP) validated tool to monitor configurations of Windows XP and Windows Vista computers.**

Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle.

Related Security Controls: CA-2, CA-4, CA-5, CA-6, CM-4.

Low	Moderate	High
CA-7 (2)	CA-7 (2)	CA-7(1)(2)

6. **CONFIGURATION MANAGEMENT CONTROLS**. Configuration Management (CM) applies administration, technical direction, and surveillance to identify and document functional and physical characteristics of a configuration item, control changes, record and report change processing and implementation, and verify compliance with specified requirements. It also provides for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP)800-70, Security Configuration Checklists Program for IT Products—Guidance for Checklist Users and Developers, and addresses ***the Federal Desktop Core Configuration (FDCC) mandated by OMB.***

Table 6. Configuration Management Controls

Configuration Management				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
CM-1	Configuration Management Policy and Procedures	CM-1(2)	CM-1 (1)(2)	CM-1 (1)(2)
CM-2	Baseline Configuration	CM-2(3)	CM-2 (1)(3)	CM-2 (1)(2)(3)
CM-3	Configuration Change Control	CM-3	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	CM-4(1)	CM-4(1)	CM-4(1)
CM-5	Access Restrictions for Change	CM-5	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6 (2)(3)	CM-6 (2)(3)(4)	CM-6 (1)(2)(3)
CM-7	Least Functionality	CM-7	CM-7	CM-7 (1)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1)(2)

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements:

(1) **Configuration management for information systems includes the following:**

- **Information system and configuration item unique identification and labeling**
- **Design documentation, including system specification and configuration item specifications**
- **Configuration change identification, tracking, control, and history**
- **Configuration status accounting to track changes from identification to implementation to produce a new baseline**
- **Security configuration checklist for operating system software, application software, and hardware platforms**
- **Configuration auditing to trace modifications to configuration items for authorized changes**

(2) **Configuration management for information systems includes adoption of the Federal Desktop Core Configurations (FDCC).**

Low	Moderate	High
CM-1(2)	CM-1 (1)(2)	CM-1 (1)(2)

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains a current baseline configuration of the information system.

Supplemental Guidance: This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the **DOE** Enterprise Architecture.

Related Security Controls: CM-6, CM-8.

Control Enhancements:

(1) The organization updates the baseline configuration of the information system as an integral part of information system component installations.

(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

(3) **The information system baseline configuration includes the following documentation:**

- **system security plan (SSP),**
- **contingency plan,**
- **user and administrator guidance,**
- **system component inventory,**
- **configuration management plan (CMP), and**
- **security testing and evaluation (assessment) procedures.**

Low	Moderate	High
CM-2 (3)	CM-2 (1)(3)	CM-2 (1)(2)(3)

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization authorizes, documents, and controls changes to the information system.

Supplemental Guidance: The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications.

Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system.

Related Security Controls: CM-4, CM-6, SI-2.

Control Enhancements:

(1) The organization employs automated mechanisms to:

- document proposed changes to the information system,
- notify appropriate approval authorities,
- highlight approvals that have not been received in a timely manner,
- inhibit change until necessary approvals are received; and,
- document completed changes to the information system.

Low	Moderate	High
CM-3	CM-3	CM-3 (1)

CM-4 MONITORING CONFIGURATION CHANGES

Control: The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.

Supplemental Guidance: Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security

features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system.

Related Security Control: CA-7.

Control Enhancements:

(1) **Security Content Automation Protocol (SCAP) validated tool(s) is used to monitor compliance of information systems against the FDCC standard configuration baseline(s).**

Low	Moderate	High
CM-4(1)	CM-4(1)	CM-4(1)

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization:

- approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system and
- generates, retains, and reviews records reflecting all such changes.

Supplemental Guidance: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

Control Enhancements:

(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

Low	Moderate	High
CM-5	CM-5	CM-5 (1)

CM-6 CONFIGURATION SETTINGS

Control: The organization:

- establishes mandatory configuration settings for information technology products employed within the information system,
- configures the security settings of information technology products to the most restrictive mode consistent with operational requirements,
- documents the configuration settings, and
- enforces the configuration settings in all components of the information system.

Supplemental Guidance: Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems.

Related Security Controls: CM-2, CM-3, SI-4.

Control Enhancements:

(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

(2) **Organizations using Microsoft Windows XPTM or VistaTM implement the minimum common Federal security configurations (Federal Desktop Core Configuration [FDCC]) available from NIST[2]:**

(a) **Organizations document deviations from the FDCC.**

(b) **Organizations map each computer using Windows XP and/or Vista to one of the following five environments/system roles:**

1 **Centrally Managed General Purpose Desktop - The desktop systems run end-user productivity applications (e.g., email clients, word processors). The desktop systems are joined to a native Windows active directory environment where the policy is managed through Microsoft Group Policy Objects (GPO).**

[2] The Microsoft Windows XP and Vista security configurations are available at http://fdcc.nist.gov/download_fdcc.html.

2 **Centrally Managed General Purpose Laptop - laptop systems run end-user productivity applications (e.g., email clients, word processors). The laptop systems are joined to a native Windows active directory environment where the policy is managed through GPOs.**

3 **Development System - The systems are used to perform development-related tasks.**

4 **Special Use System - The systems perform a special task that does not fit into any of the above categories (e.g., laboratory/research systems, kiosk systems, SCADA systems).**

5 **Other - The systems cannot be grouped into any of the above categories. This includes desktops and laptops that are not centrally managed.**

(3) **Minimum Security Configurations other than Microsoft Windows XP™ or Vista™ are selected from recognized sources of checklist-producing organizations, including NIST[3], the National Security Agency (NSA)[4], the Defense Information Systems Agency (DISA) [5] Security Technical Implementation Guides (STIGs), and the Center for Internet Security (CIS) benchmarks.[6]**

(4) **DAA-approval for configuration settings to enable the automatic execution of programs and processes on removable media, such as Microsoft Auto Run.**

Low	Moderate	High
CM-6 (2)(3)	CM-6 (2)(3)	CM-6 (1)(2)(3)

CM-7 LEAST FUNCTIONALITY

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services* ***documented in the information system SSP***].

[3] The NIST checklist repository is located at http://checklists.nist.gov/ .
[4] The NSA's checklists are available at http://www.nsa.gov/ia/.
[5] DISA's STIGs are available at http://iase.disa.mil/stigs/index.html.
[6] CIS's site is http://www.cisecurity.org/.

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., voice over internet protocol, instant messaging, file transfer protocol, hyper text transfer protocol, file sharing). **The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.**

Control Enhancements:

(1) The organization reviews the information system [*Assignment: organization-defined frequency, **at least annually***] to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Low	Moderate	High
CM-7	CM-7	CM-7 (1)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.

Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system.

Related Security Controls: CM-2, CM-6.

Control Enhancements:

(1) The organization updates the inventory of information system components as an integral part of component installations.

(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Low	Moderate	High
CM-8	CM-8 (1)	CM-8 (1)(2)

7. CONTINGENCY PLANNING CONTROLS. Contingency Planning details the necessary procedures required to protect the continuing performance of core business functions and services, including information and information system services, during an outage**.**

Table 7. Contingency Planning Controls

Contingency Planning				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1)(2)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)(2)
CP-4	Contingency Plan Testing	CP-4	CP-4(1)	CP-4 (1)(2)(3)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Sites	Not Selected	CP-6 (1)(3)	CP-6 (1)(2)(3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1)(2)(3)	CP-7 (1)(2)(3)(4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1)(2)	CP-8 (1)(2)(3)(4)
CP-9	Information System Backup	CP-9	CP-9 (1)(4)	CP-9 (1)(2)(3)(4)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-34 provides guidance on contingency planning. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
CP-1	CP-1	CP-1

CP-2 CONTINGENCY PLAN

Control: The organization develops, and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include business continuity plan, disaster recovery plan, continuity of operations plan, business recovery plan, incident response plan, and emergency action plan.

(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

Low	Moderate	High

Low	Moderate	High
CP-2	CP-2 (1)	CP-2 (1)(2)

CP-3 CONTINGENCY TRAINING

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

Low	Moderate	High
Not Selected	CP-3	CP-3 (1)(2)_

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization:

- tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan and

- reviews the contingency plan test/exercise results and initiates corrective actions.

Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Control Enhancements:

(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans

Enhancement Supplemental Guidance: Examples of related plans include business continuity plan, disaster recovery plan, continuity of operations plan, business recovery plan, incident response plan, and emergency action plan.

(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

(3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.

Low	Moderate	High
CP-4	CP-4(1)	CP-4 (1)(2)(3)

CP-5 CONTINGENCY PLAN UPDATE

Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Supplemental Guidance: Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., business continuity plan, disaster recovery plan, continuity of operations plan, business recovery plan, incident response plan, emergency action plans).

Control Enhancements: None.

Low	Moderate	High
CP-5	CP-5	CP-5

CP-6 ALTERNATE STORAGE SITE

Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Control Enhancements:

(1) The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.

(2) The organization configures the alternate storage site to facilitate timely and effective recovery operations.

(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Low	Moderate	High
Not Selected	CP-6 (1)(3)	CP-6 (1)(2)(3)

CP-7 ALTERNATE PROCESSING SITE

Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*Assignment: organization-defined time period, **in a timely manner as specified in the information system SSP***], when the primary processing capabilities are unavailable.

Supplemental Guidance: Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives.

Control Enhancements:

(1) The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.

(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(4) The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.

Low	Moderate	High
Not Selected	CP-7 (1)(2)(3)	CP-7 (1)(2)(3)(4)

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*Assignment: organization-defined time period,* ***in a timely manner, as specified by the operating unit***], when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).

Control Enhancements:

(1) The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(2) The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.

(3) The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

(4) The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.

Low	Moderate	High
Not Selected	CP-8 (1)(2)	CP-8 (1)(2)(3)(4)

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*, ***at least annually***] and protects backup information at the storage location.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control.

Related Security Controls: MP-4, MP-5.

Control Enhancements:

(1) The organization tests backup information [*Assignment: organization-defined frequency*, ***at least annually***] to verify media reliability and information integrity.

(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.

(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

(4) The organization protects system backup information from unauthorized modification.

Enhancement Supplemental Guidance: The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control.

Related Security Controls: MP-4, MP-5.

Low	Moderate	High
CP-9	CP-9 (1)(4)	CP-9 (1)(2)(3)(4)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

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

Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Control Enhancements:

(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.

Low	Moderate	High
CP-10	CP-10	CP-10 (1)

8. IDENTIFICATION AND AUTHENTICATION CONTROLS. Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an information system. Access control usually requires that the system be able to identify and differentiate among users. All DOE information systems must have means to enforce user accountability, so that system activity (both authorized and unauthorized) can be traced to a specific user. To facilitate user accountability, all information systems will implement user identification and authentication methods. The user identification tells the system who the user is. The authentication mechanism provides an added level of assurance that the user really is who they say they are. Authentication consists of something a user knows (such as a password), something the user has (such as a token or smart card), or something the user is (such as a fingerprint). User identification and authentication also can enforce separation of duties.

Table 8. Identification and Authentication Controls

Identification and Authentication				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2(2)	IA-2 (1)(2)(4)	IA-2 (2)(3)(4)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5 (1)(2)(3)(4)(5) (6)(7)(8)(9)	IA-5 (1)(2)(3)(4)(5) (6)(7)(8)(9)	IA-5 (1)(2)(3)(4)(5) (6)(7)(8)(9)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: The identification and authentication policy and procedures are consistent with:

- FIPS 201 and SPs 800-73, 800-76, and 800-78 and
- other applicable laws, Executive orders, directives, policies, regulations, standards, and guidance.

NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

Low	Moderate	High
IA-1	IA-1	IA-1

IA-2 USER IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multi-factor authentication, some combination thereof.

NIST SP 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in SP 800-63 is applied to both local and remote access to information systems.

Remote access is any access to an organizational information system by a user (or an information system) communicating through **the accreditation boundary of the information system**. Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network.

Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST SP 800-63 level 1 compliant. FIPS 201 and SPs 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. **DOE N 206.4, *Personal Identity Verification*, also contains DOE requirements related to authorization credentials and their issuance.**

In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication

risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST SP 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals.

Related Security Controls: AC-14, AC-17.

Control Enhancements:

(1) The information system employs multi-factor authentication for remote system access that is NIST SP 800-63 [*Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4*] compliant.

(2) The information system employs multi-factor authentication for local system access that is NIST SP 800-63 [*Selection: organization-defined level 3 or level 4*] compliant.

(3) The information system employs multi-factor authentication for remote system access that is NIST SP 800-63 level 4 compliant.

(4) **Multi-factor authentication process is mandatory for system administrator and privileged user access to systems where passwords are used as one authentication method.**

Low	Moderate	High
IA-2(2)	IA-2 (1)(2)(4)	IA-2 (2)(3)(4)

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system identifies and authenticates specific devices before establishing a connection.

Supplemental Guidance: The information system typically uses either shared known information [e.g., media access control (MAC) or transmission control protocol/internet protocol (TCP/IP) addresses] or an organizational authentication solution [e.g., IEEE 802.1x and extensible authentication protocol (EAP) or a Radius server with EAP-transport layer security (TLS) authentication] to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Control Enhancements: None.

Low	Moderate	High
Not Selected	IA-3	IA-3

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages user identifiers by:

- uniquely identifying each user **or group**,
- verifying the identity of each user,
- receiving authorization to issue a user identifier from an appropriate organization official,
- issuing the user identifier to the intended party,
- disabling the user identifier after [*Assignment: organization-defined time period*] of inactivity, and
- archiving user identifiers.

Supplemental Guidance: Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and SPs 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. **DOE N 206.4, *Personal Identity Verification,* also contains DOE requirements related to authorization credentials and their issuance.**

Control Enhancements: None.

Low	Moderate	High
IA-4	IA-4	IA-4

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by:

- defining initial authenticator content;
- establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;
- changing default authenticators upon information system installation;

- changing/refreshing authenticators periodically; and

- **providing a user authentication mechanism on all information systems that is unique to each user, such as but not limited to; passwords, one-time passwords, biometrics, or public-key infrastructure certificates for primary access to all information and information system resources.**

Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system:

- protects passwords from unauthorized disclosure and modification when stored and transmitted,

- prohibits passwords from being displayed when entered,

- enforces password minimum and maximum lifetime restrictions

- prohibits password reuse for a specified number of generations**, and**

- **prevents the use of expired passwords.**

For PKI-based authentication, the information system:

- validates certificates by constructing a certification path to an accepted trust anchor,

- establishes user control of the corresponding private key, and

- maps the authenticated identity to the user account.

In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and NIST SPs 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST SP 800-63 provides guidance on remote electronic authentication. **DOE N 206.4, *Personal Identity Verification*, also contains DOE requirements related to authorization credentials and their issuance.**

Control Enhancements:

(1) **A minimum of four-character passwords are used on personal digital assistants (PDAs).**

(2) **Passwords are prohibited from being transmitted between systems in clear text.**

(3) **Passwords for servers, mainframes, desktops/workstations, telecommunications devices (such as routers and switches), and devices used for cyber security functions (such as firewalls, intrusion detection, and audit logging) are encrypted with DAA-approved encryption when stored electronically.**

(4) **User-created authenticators on unclassified information systems are different from those employed by the same user on National Security Systems.**

(5) **Users are notified when their passwords/pass codes will expire and must be changed to continue access to the information system or lockout will occur.**

(6) **Passwords and pass phrases are changed from those supplied by the vendor prior to first operational use or connection to a network; changed at least every 6 months; changed immediately after sharing; changed immediately after an actual or suspected compromise; and changed on direction from management.**

(7) **Group passwords (i.e., a single password used by a group of users) are used only with additional mechanisms that can assure accountability (such as separate and unique User IDs).**

(8) **Authenticator generation and verification software generates/verifies a pass phrase containing at least 25 characters or passwords in accordance with the following criteria.**

- **Passwords contain at least eight non-blank characters.**
- **Passwords contain a combination of letters, numbers, and at least one special character.**
- **Passwords do not contain the user identification (userid).**
- **Passwords do not contain any common English dictionary words, spelled forward or backwards (except words of three or fewer characters);**
- **Passwords do not employ common names.**

- **Passwords do not contain any commonly used numbers (e.g., the employee serial number, Social Security number, birth date, phone number) associated with the user of the password.**

- **Passwords do not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx."**

(9) **The implementation of authentication technology provides access security commensurate with the level of sensitivity assigned to the resource (i.e. information, devices or systems).**

Low	Moderate	High
IA-5 (1)(2)(3)(4)(5)(6)(7)(8)(9)	IA-5 (1)(2)(3)(4)(5)(6)(7)(8)(9)	IA-5 (1)(2)(3)(4)(5)(6)(7)(8)(9)

IA-6 AUTHENTICATOR FEEDBACK

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

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Control Enhancements: None.

Low	Moderate	High
IA-6	IA-6	IA-6

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Control Enhancements: None.

Low	Moderate	High
IA-7	IA-7	IA-7

9. **INCIDENT RESPONSE CONTROLS.** An incident response capability is a mechanism through which an operating unit's system owners and Information System Security Officers are kept informed of system vulnerability advisories from the US-Computer Emergency Readiness Team (US-CERT), software vendors, and other sources. The capability also coordinates with responsible incident response capabilities regarding the handling and reporting of incidents involving systems under the operating unit's responsibility. An incident response capability may consist of one or more persons (such as the Information System Security Officer or CIO), who ensure that vulnerability advisories are communicated to system owners.

Table 9. Incident Response Controls

Incident Response				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1)
IR-3	Incident Response Testing	IR-3	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	IR-5(2)	IR-5(2)	IR-5 (1)(2)
IR-6	Incident Reporting	IR-6(2)	IR-6 (1)(2)	IR-6 (1)(2)
IR-7	Incident Response Assistance	IR-7(2)	IR-7 (1)(2)	IR-7 (1)(2)

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational and Departmental entities, and compliance and
- formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Supplemental Guidance: The incident response policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations,

standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

Control Enhancements: None.

Low	Moderate	High
IR-1	IR-1	IR-1

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

Low	Moderate	High
IR-2	IR-2	IR-2 (1)

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Control: The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: **tests and exercises defined in the information system SSP***] to determine the incident response effectiveness and documents the results.

Supplemental Guidance: NIST SP 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Control Enhancements:

(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.

Low	Moderate	High
IR-3	IR-3	IR-3 (1)

IR-4 INCIDENT HANDLING

Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery i**n accordance with DOE requirements**.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.

Related Security Controls: AU-6, PE-6.

Control Enhancements:

(1) The organization employs automated mechanisms to support the incident handling process.

Low	Moderate	High
IR-4	IR-4 (1)	IR-4 (1)

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents on an ongoing basis.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

(2) **The organization employs Department level resources to monitor for incidents (e.g., Cooperative Protection Program [CPP]).**

Low	Moderate	High
IR-5(2)	IR-5(2)	IR-5 (1)(2)

IR-6 INCIDENT REPORTING

Control: The organization promptly reports incident information **in accordance with DOE requirements**.

Supplemental Guidance: The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-61 provides guidance on incident reporting.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

(2) **The organization reports incidents and potential incidents to Operating Unit management.**

Low	Moderate	High
IR-6(2)	IR-6 (1)(2)	IR-6 (1)(2)

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

Control Enhancements:

(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.

(2) **The organization employs Departmental level resources for incident forensics analysis (e.g., Cyber Forensics Laboratory).**

Low	Moderate	High
IR-7(2)	IR-7 (1)(2)	IR-7 (1)(2)

10. **MAINTENANCE CONTROLS**. These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. The process of configuration management provides for a controlled environment in which changes to hardware and software are properly authorized, tested, and approved before implementation.

Table 10. Maintenance Controls

Maintenance				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Periodic Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1)(2)(3)
MA-4	Remote Maintenance	MA-4	MA-4 (1)(2)	MA-4 (1)(2)(3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: The information system maintenance policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
MA-1	MA-1	MA-1

MA-2 CONTROLLED MAINTENANCE

Control: The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Supplemental Guidance: All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Control Enhancements:

(1) The organization maintains maintenance records for the information system that include:

- the date and time of maintenance;
- name of the individual performing the maintenance;
- name of escort, if necessary;
- a description of the maintenance performed; and
- a list of equipment removed or replaced (including identification numbers, if applicable).

(2) The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to date, accurate, complete, and available records of all maintenance actions, both needed and completed.

Low	Moderate	High
MA-2	MA-2 (1)	MA-2 (1) (2)

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.

Supplemental Guidance: The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Control Enhancements:

(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

(3) The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.

(4) The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

Low	Moderate	High
Not Selected	MA-3	MA-3 (1)(2)(3)

MA-4 REMOTE MAINTENANCE

Control: The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.

Supplemental Guidance: Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include:

- encryption and decryption of communications;
- strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST SP 800-63; and
- remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity.

If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST SP 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Related Security Controls: IA-2, MP-6.

Control Enhancements:

(1) The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.

(2) The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.

(3) The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.

Low	Moderate	High
MA-4	MA-4 (1)(2)	MA-4 (1)(2)(3)

MA-5 MAINTENANCE PERSONNEL

Control: The organization allows only authorized personnel to perform maintenance on the information system.

Supplemental Guidance: Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Control Enhancements: None.

Low	Moderate	High
MA-5	MA-5	MA-5

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and spare parts for [*Assignment: organization-defined list of key information system components*] within [*Assignment: organization-defined time period, **a time frame to support mission requirements***] of failure.

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
Not Selected	MA-6	MA-6

11. **MEDIA PROTECTION CONTROLS**. DOE, including NNSA, requires that operating unit cyber security programs include procedures for storing, handling, and destroying national and non-national security information media.

Table 11. Media Protection Controls

Media Protection		
Control	**Control Name**	**Control Baselines**

Number		Low	Moderate	High
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2(1)	MP-2 (1)
MP-3	Media Labeling	Not Selected	MP-3	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (1)(2)	MP-5 (1)(2)(3)
MP-6	Media Sanitization and Disposal	MP-6	MP-6 (1)(2)	MP-6 (1)(2)

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: The media protection policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
MP-1	MP-1	MP-1

MP-2 MEDIA ACCESS

Control: The organization restricts access to information system media to authorized individuals.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access.

Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Control Enhancements:

(1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Enhancement Supplemental Guidance: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

Low	Moderate	High
MP-2	MP-2(1)	MP-2 (1)

MP-3 MEDIA LABELING

Control: The organization:

- affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information and

- exempts [*Assignment: organization-defined list of media types,* ***documented the specific types of media or hardware components in the information system SSP***] exempt from labeling so long as they remain within [*Assignment: organization-defined protected environment*].

Supplemental Guidance: An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information

contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Control Enhancements: None.

Low	Moderate	High
Not Selected	MP-3	MP-3

MP-4 MEDIA STORAGE

Control: The organization physically controls and securely stores information system media within controlled areas.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices.

FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST SPs 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management.

Related Security Controls: CP-9, RA-2.

Control Enhancements: None.

Low	Moderate	High
Not Selected	MP-4	MP-4

MP-5 MEDIA TRANSPORT

Control: The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate

storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Control Enhancements:

(1) The organization protects digital and non-digital media during transport outside of controlled areas using [*Assignment: organization-defined security measures, e.g., locked container, cryptography*].

Enhancement Supplemental Guidance: Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used.

(2) The organization documents, where appropriate, activities associated with the transport of information system media using [*Assignment: organization-defined system of records*].

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

(3) The organization employs an identified custodian at all times to transport information system media.

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

Low	Moderate	High
Not Selected	MP-5 (1)(2)	MP-5 (1)(2)(3)

MP-6 MEDIA SANITIZATION AND DISPOSAL

Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse **in accordance with DOE requirements.**

Supplemental Guidance: Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging,

and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed.

The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed.

Control Enhancements:

(1) The organization tracks, documents, and verifies media sanitization and disposal actions.

(2) The organization periodically tests sanitization equipment and procedures to verify correct performance.

Low	Moderate	High
MP-6	MP-6	MP-6 (1)(2)

12. **PHYSICAL AND ENVIRONMENTAL PROTECTION**. Measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Physical and Environment Physical controls include: (i) limiting physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protecting the physical building and support infrastructure for information systems; (iii) providing supporting utilities for information systems; and (iv) protecting information systems against environmental hazards.

Table 12. Physical and Environmental Protection Controls

Physical and Environmental Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	PE-4	PE-4
PE-5	Access Control for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6 (3)	PE-6 (1)(3)	PE-6 (1) (2)(3)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Logs	PE-8	PE-8	PE-8 (1)(2)

Physical and Environmental Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10 (1)	PE-10 (1)
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1)(2)(3)	PE-13 (1)(2)(3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18(1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and
- formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: The physical and environmental protection policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
PE-1	PE-1	PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides. **DOE M 470.4-2, *Physical Protection*, and DOE N 206.4, *Personal Identity Verification*, also contain DOE requirements related to authorization credentials and their issuance.**

Control Enhancements: None.

Low	Moderate	High
PE-2	PE-2	PE-2

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Supplemental Guidance: The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys:

- periodically and
- when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where

federal personal identity verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST SP 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST SP 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST SP 800-76. **DOE N 206.4, *Personal Identity Verification*, also contains DOE requirements related to authorization credentials and their issuance.**

Control Enhancements:

(1) The organization controls physical access to the information system independent of the physical access controls for the facility.

Enhancement Supplemental Guidance: This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.

Low	Moderate	High
PE-3	PE-3	PE-3 (1)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include:

- locked wiring closets,
- disconnected or locked spare jacks, and/or
- protection of cabling by conduit or cable trays.

Control Enhancements: None.

Low	Moderate	High
Not Selected	PE-4	PE-4

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM

Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
Not Selected	PE-5	PE-5

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization monitors physical access to the information system to detect and respond to physical security incidents.

Supplemental Guidance: The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.

Control Enhancements:

(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.

(3) Portable/mobile devices used to process sensitive unclassified information (SUI), including personally identifiable information or in any area where SUI is processed and taken outside the United States, other than the assigned user's primary work location, are sealed with Senior DOE Management-approved tamper-indicating devices, or DAA-approved alternative protection measures, prior to removal of the computing device from the user's primary location.

Low	Moderate	High

Low	Moderate	High
PE-6 (3)	PE-6 (1)(3)	PE-6 (1) (2)(3)

PE-7 VISITOR CONTROL

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Supplemental Guidance: Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST SP 800-79. **DOE N 206.4, *Personal Identity Verification*, also contains DOE requirements related to authorization credentials and their issuance.**

Control Enhancements:

(1) The organization escorts visitors and monitors visitor activity, when required.

Low	Moderate	High
PE-7	PE-7 (1)	PE-7 (1)

PE-8 ACCESS RECORDS

Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes:

- name and organization of the person visiting,
- signature of the visitor,
- form of identification,
- date of access,
- time of entry and departure,
- purpose of visit, and
- name and organization of person visited. Designated officials within the organization review the visitor access records [*Assignment: organization-defined frequency**, in a timely manner after closeout of the visitor access record, as specified by the operating unit***].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.

(2) The organization maintains a record of all physical access, both visitor and authorized individuals.

Low	Moderate	High
PE-8	PE-8	PE-8 (1)(2)

PE-9 POWER EQUIPMENT AND POWER CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths.

Low	Moderate	High
Not Selected	PE-9	PE-9

PE-10 EMERGENCY SHUTOFF

Control: The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

Supplemental Guidance: Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Control Enhancements:

(1) The organization protects the emergency power-off capability from accidental or unauthorized activation.

Low	Moderate	High
Not Selected	PE-10 (1)	PE-10 (1)

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

Low	Moderate	High
Not Selected	PE-11	PE-11 (1)

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
PE-12	PE-12	PE-12

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

Supplemental Guidance: Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control Enhancements:

(1) The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.

(2) The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.

(3) The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

Low	Moderate	High
PE-13	PE-13 (1)(2)(3)	PE-13 (1)(2)(3)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
PE-14	PE-14	PE-14

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.

Low	Moderate	High
PE-15	PE-15	PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.

Supplemental Guidance: The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.

Control Enhancements: None.

Low	Moderate	High
PE-16	PE-16	PE-16

PE-17 ALTERNATE WORK SITE

Control: The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Supplemental Guidance: The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST SP 800-46 provides guidance on security in telecommuting and broadband communications.

Control Enhancements: None.

Low	Moderate	High
Not Selected	PE-17	PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever

possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Control Enhancements:

(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

Low	Moderate	High
Not Selected	PE-18	PE-18(1)

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	Not Selected

13. **PLANNING CONTROLS**. Planning is the process of developing, documenting, periodically updating, and implementing security plans for information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems

Table 13. Planning Controls

Planning				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4 (1)	PL-4 (1)	PL-4 (1)

Planning				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security Related Activity Planning	PL-6	PL-6	PL-6

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: The security planning policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-18 provides guidance on security planning. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
PL-1	PL-1	PL-1

PL-2 SYSTEM SECURITY PLAN

Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

Supplemental Guidance: The security plan is aligned with the organization's information system architecture and information security architecture. NIST SP 800-18 provides guidance on security planning.

Control Enhancements: None.

Low	Moderate	High
PL-2	PL-2	PL-2

PL-3 SYSTEM SECURITY PLAN UPDATE

Control: The organization reviews the security plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

Supplemental Guidance: Significant changes are defined in advance by the organization and identified in the configuration management process. NIST SP 800-18 provides guidance on security plan updates.

Control Enhancements: None.

Low	Moderate	High
PL-3	PL-3	PL-3

PL-4 RULES OF BEHAVIOR

Control: The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Supplemental Guidance: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST SP 800-18 provides guidance on preparing rules of behavior.

Control Enhancements:

(1) **The organization establishes rules of behavior and operations and consequences for violating policy and procedures.**

Low	Moderate	High
PL-4 (1)	PL-4 (1)	PL-4 (1)

PL-5 PRIVACY IMPACT ASSESSMENT

Control: The organization conducts a privacy impact assessment on the information system in accordance with **[*Assignment: organization-defined processes for implementing OMB and Departmental policy*]**.

b. *Supplemental Guidance*: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002. **Departmental procedures for implementing OMB M-03-22 are defined in** requirements defined by the Senior Agency Official for Privacy.

Control Enhancements: None.

Low	Moderate	High
PL-5	PL-5	PL-5

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Supplemental Guidance: Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Control Enhancements: None.

Low	Moderate	High
PL-6	PL-6	PL-6

14. **PERSONNEL SECURITY CONTROLS**. Effective administration of users' computer access is essential to maintaining system security. Administration of system users focuses on identification, authentication, and access authorizations. DOE, including NNSA, requires that each operating unit implement and maintain a process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations. In addition, they are to address the timely modification or removal of access and associated issues for employees who are reassigned, promoted, or terminated. Many important issues in computer security involve Federal and contractor system users, designers/programmers, implementers/maintainers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their job. No computer system can be secured without properly addressing these security issues.

Table 14. Personnel Security Controls

Personnel Security				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2 (1)	PS-2 (1)
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: The personnel security policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
PS-1	PS-1	PS-1

PS-2 POSITION CATEGORIZATION

Control: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. **The position functions/capabilities/authorities include:**

- **Positions (users) with cyber security authority, "root" access to systems, or access to software source code who have opportunity to bypass system security control settings – for example, network/system administrator, system developer, and cyber security program positions (such as ISSOs and cyber security managers).**

- **Positions (users) with access to an operating unit local area network, e-mail, basic office applications (such as Microsoft Office or Corel Office suites), and their own personal data records (i.e., only personal/private information pertaining to themselves such as their personal time and attendance record or Thrift Savings Plan account).**

The organization reviews and revises position risk designations [*Assignment: organization-defined frequency,* ***at least every 3 years***].

Supplemental Guidance: Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance. **The position categorization is based on the sensitivity of the information to be handled, sensitivity of the system, or the risk and magnitude of loss or harm that could be caused by the individual.**

Related Security Controls: PS-3.

Control Enhancements:

(1) **The position functions/capabilities/authorities include positions (users) with root access that may modify core data stores of information systems, users with authority to electronically approve financial transactions, or users with access to personal/Privacy Act/other protected data (e.g., social security numbers in human resource systems, etc.) other than their own**.

Low	Moderate	High
PS-2	PS-2(1)	PS-2(1)

PS-3 PERSONNEL SCREENING

Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access. **Screening will be performed for operating unit employees, contractors, and any "guests" prior to their being given access to operating unit systems and networks.**

Supplemental Guidance: Screening is consistent with:

- 5 CFR 731.106;

- Office of Personnel Management policy, regulations, and guidance;
- organizational policy, regulations, and guidance;
- FIPS 201 and SPs 800-73, 800-76, and 800-78; and
- the criteria established for the risk designation of the assigned position.

The level of screening required varies from minimal checks to a full background investigation depending the position categorization. DOE N 206.4, *Personal Identity Verification*, also contains requirements for personnel screening related to issuing DOE security badges.

Related Security Controls: PS-2.

Control Enhancements: None.

Low	Moderate	High
PS-3	PS-3	PS-3

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

Supplemental Guidance: Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

Low	Moderate	High
PS-4	PS-4	PS-4

PS-5 PERSONNEL TRANSFER

Control: The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.

Supplemental Guidance: Appropriate actions that may be required include:

- returning old and issuing new keys, identification cards, building passes;
- closing old accounts and establishing new accounts;
- changing system access authorizations; and
- providing for access to official records created or controlled by the employee at the old work location and in the old accounts.

Control Enhancements: None.

Low	Moderate	High
PS-5	PS-5	PS-5

PS-6 ACCESS AGREEMENTS

Control: The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Control Enhancements: None.

Low	Moderate	High
PS-6	PS-6	PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST SP 800-35 provides guidance on information technology security services.

Control Enhancements: None.

Low	Moderate	High
PS-7	PS-7	PS-7

PS-8 PERSONNEL SANCTIONS

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Control Enhancements: None.

Low	Moderate	High
PS-8	PS-8	PS-8

15. **RISK ASSESSMENT CONTROLS**. Risk measures the combined results of threat likelihood of occurrence and level of impact on Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. Risk management is the ongoing process of managing risks to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; the selection, implementation, and assessment of cost-effective security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

A system owner, in consultation with the information system security officer and other interested parties, such as the designated approving authority, uses the results of this evaluation to determine countermeasures to prevent or mitigate risk to an acceptable level. The information system security officer can assist by providing the system owner with a risk assessment methodology and by providing assistance in interpreting the risk assessment results and suggesting possible cost-effective security countermeasure alternatives. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance, best practices, and sample templates for the risk assessment process.

Table 15. Controls for Risk Assessment

Risk Assessment				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High

Risk Assessment				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	RA-5	RA-5 (1)	RA-5 (1) (2)

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: The risk assessment policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-30 provides guidance on the assessment of risk. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
RA-1	RA-1	RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

Supplemental Guidance: The applicable federal standard for security categorization of non-national security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST SP 800-60 provides guidance on determining the security categories of the information types resident on the information system.

Related Security Controls: MP-4, SC-7, E-SU-4.

Control Enhancements: None.

Low	Moderate	High
RA-2	RA-2	RA-2

RA-3 RISK ASSESSMENT

Control: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

Supplemental Guidance: Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such,

organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST SP 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Control Enhancements: None.

Low	Moderate	High
RA-3	RA-3	RA-3

RA-4 RISK ASSESSMENT UPDATE

Control: The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

Supplemental Guidance: The organization develops and documents specific criteria for what is considered significant change to the information system. NIST SP 800-30 provides guidance on conducting risk assessment updates.

Control Enhancements: None.

Low	Moderate	High
RA-4	RA-4	RA-4

RA-5 VULNERABILITY SCANNING

Control: The organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency, **at least quarterly***] or when significant new vulnerabilities potentially affecting the system are identified and reported.

Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST SP 800-42 provides guidance

on network security testing. NIST SP 800-40 (Version 2) provides guidance on patch and vulnerability management.

Control Enhancements:

(1) The organization employs vulnerability scanning tools [*Assignment: organization-defined frequency*, ***at least quarterly***] that include the capability to readily update the list of information system vulnerabilities scanned.

(2) The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*, ***at least quarterly***] or when significant new vulnerabilities are identified and reported.

(3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.

Low	Moderate	High
RA-5	RA-5 (1)	RA-5 (1) (2)

16. **SYSTEM AND SERVICES ACQUISITION CONTROLS**. Allocating resources to protect systems, employing system development life cycles processes, employing software usage and installation restrictions, and ensuring that third-party providers employ adequate security measures to protect outsourced information, applications, or services.

Table 16. Systems and Services Acquisition Controls

System and Services Acquisition				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4(3)	SA-4 (1)(3)	SA-4 (1)(3)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1)(2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8

System and Services Acquisition				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SA-9	External Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: The system and services acquisition policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
SA-1	SA-1	SA-1

SA-2 ALLOCATION OF RESOURCES

Control: The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

Supplemental Guidance: The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budget documentation. NIST SP 800-65 provides guidance on integrating security into the capital planning and investment control process.

Control Enhancements: None.

Low	Moderate	High
SA-2	SA-2	SA-2

SA-3 LIFE CYCLE SUPPORT

Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations.

Supplemental Guidance: NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

Control Enhancements: None.

Low	Moderate	High
SA-3	SA-3	SA-3

SA-4 ACQUISITIONS

Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system **and information technology services** acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive orders, directives, policies, regulations, and standards.

Supplemental Guidance:

- *Solicitation Documents*. The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe:
  - required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements);
  - required design and development processes;

- required test and evaluation procedures; and
- required documentation.

The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST SP 800-36 provides guidance on the selection of information security products. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on security considerations in the system development life cycle.

- *Information System Documentation*. The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

- *Use of Tested, Evaluated, and Validated Products*. NIST SP 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.

- *Configuration Settings and Implementation Guidance*. The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST SP 800-70 provides guidance on configuration settings for information technology products.

Control Enhancements:

(1) The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

(2) The organization requires in solicitation documents that appropriate documentation be provided describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components **and common security configurations).**

(3) The organization requires the provider of information technology to certify that applications are fully functional and operate correctly as

intended on information systems using the minimum security standard configuration.

Low	Moderate	High
SA-4(3)	SA-4 (1)(3)	SA-4 (1)(3)

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.

Supplemental Guidance: Documentation includes administrator and user guides with information on:

- configuring, installing, and operating the information system and
- effectively using the system's security features.

When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Control Enhancements:

(1) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

(2) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

Low	Moderate	High
SA-5	SA-5 (1)	SA-5 (1)(2)

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: The organization complies with software usage restrictions.

Supplemental Guidance: Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Control Enhancements: None.

Low	Moderate	High
SA-6	SA-6	SA-6

SA-7 USER INSTALLED SOFTWARE

Control: The organization enforces explicit rules governing the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Control Enhancements: None.

Low	Moderate	High
SA-7	SA-7	SA-7

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization designs and implements the information system using security engineering principles.

Supplemental Guidance: NIST SP 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SA-8	SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:

- requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive orders, directives, policies, regulations, standards, guidance, and established service-level agreements and
- monitors security control compliance.

Supplemental Guidance: An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials will require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST SP 800-35 provides guidance on information technology security services. NIST SP 800-64 provides guidance on the security considerations in the system development life cycle.

Control Enhancements: None.

Low	Moderate	High
SA-9	SA-9	SA-9

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

Supplemental Guidance: This control also applies to the development actions associated with information system changes.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SA-10	SA-10

SA-11 DEVELOPER SECURITY TESTING

Control: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system. *Related Security Controls*: CA-2, CA-4.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SA-11	SA-11

17. **SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS**. Monitoring, controlling and protecting communications at external and internal boundaries of information systems, and employing architectural designs, software development techniques, and systems engineering principles to promote effective security.

Table 17. System and Communications Protection Controls

System and Communications Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	SC-3	SC-3
SC-4	Information Remnants	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7 (1)(2)(3)(4)(5)(6)(7)	SC-7 (1)(2)(3)(4)(5)(6)(7)	SC-7 (1)(2)(3)(4)(5)(6)(7)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	SC-19	SC-19	SC-19
SC-20	Secure Name/Address Resolution Service (Authentication Source)	Not Selected	SC-20	SC-20
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
SC-1	SC-1	SC-1

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SC-2	SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from non-security functions.

Supplemental Guidance: The information system isolates security functions from non-security functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Control Enhancements:

(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.

(2) The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and from other security functions.

(3) The information system minimizes the number of non-security functions included within the isolation boundary containing security functions.

(4) The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.

(5) The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Low	Moderate	High
Not Selected	SC-3	SC-3

SC-4 INFORMATION REMNANCE

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to

a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SC-4	SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list,* ***as described in the information system SSP***].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

Low	Moderate	High
SC-5	SC-5	SC-5

SC-6 RESOURCE PRIORITY

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	Not Selected

SC-7 BOUNDARY PROTECTION

Control: The information system monitors and controls communications at the **accreditation** boundary of the information system and at key internal boundaries within the system.

Supplemental Guidance: Any connections to the Internet, or other external networks or information systems, occur through managed/ **controlled** interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected sub-network commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed/**controlled** interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning. **The managed/controlled interface adjudicates the difference in security policy and practices between interconnected systems and controls the flow of information between systems with differing security category impact levels.**

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-77 provides guidance on virtual private networks.

Related Security Controls: **AC-4,** MP-4, RA-2.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components to separate sub-networks with separate, physical network interfaces.

Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

(2) The organization prevents public access into the organization's internal networks except as appropriately mediated.

(3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

(4) The organization implements a managed/ **controlled** interface (boundary protection devices in effective security architecture) with any external telecommunication service **(e.g., interconnecting to systems outside of DOE, such as the Internet, public switched networks, Department of Defense, etc.)**, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

(5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

(6) 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.

(7) **All outbound network communications crossing the accreditation boundary occur through an anonymous proxy[7] service.**

Low	Moderate	High
SC-7 (1)(2)(3)(4)(5)(6)	SC-7 (1)(2)(3)(4)(5)(6)(7)	SC-7 (1)(2)(3)(4)(5)(6)(7)

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully

[7] An **anonymizer** or an **anonymous proxy** is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the internal Operating Unit's source computer's identifying information.

dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission integrity using IPsec. NIST SP 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

Low	Moderate	High
Not Selected	SC-8	SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST SP 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST SP 800-77 provides guidance on protecting transmission confidentiality using IPsec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Related Security Control: AC-17.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

Low	Moderate	High
Not Selected	SC-9	SC-9 (1)

SC-10 NETWORK DISCONNECT

Control: The information system terminates a network connection at the end of a session or after inactivity [*Assignment: organization-defined time period, **a time period specified in the information system SSP***].

Supplemental Guidance: The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SC-10	SC-10

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication*].

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	Not Selected

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

Supplemental Guidance: NIST SP 800-56 provides guidance on cryptographic key establishment. NIST SP 800-57 provides guidance on cryptographic key management.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SC-12	SC-12

SC-13 USE OF CRYPTOGRAPHY

Control: For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance.

Supplemental Guidance: The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST SPs 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Control Enhancements: None.

Low	Moderate	High
SC-13	SC-13	SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

Control: The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
SC-14	SC-14	SC-14

SC-15 COLLABORATIVE COMPUTING

Control: The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Supplemental Guidance: Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

Control Enhancements:

(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

Low	Moderate	High
Not Selected	SC-15	SC-15

SC-16 TRANSMISSION OF SECURITY PARAMETERS

Control: The information system reliably associates security parameters with information exchanged between information systems.

Supplemental Guidance: Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Control Enhancements: None.

Low	Moderate	High
Not Selected	Not Selected	Not Selected

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved,

shared service provider, as required by OMB Memorandum 05-24. NIST SP 800-32 provides guidance on public key technology. NIST SP 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SC-17	SC-17

SC-18 MOBILE CODE

Control: The organization:

- establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously and
- authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST SP 800-28 provides guidance on active content and mobile code.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SC-18	SC-18

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

- establishes usage restrictions and implementation guidance for voice over internet protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously,authorizes, monitors, and controls the use of VoIP within the information system, and
- **implements controls to reduce/eliminate the DOE TEMPEST/TSCM concerns when allowing the VOIP operation where sensitive**

unclassified and classified data are processed and verbal communication takes place.

Supplemental Guidance: NIST SP 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.

Control Enhancements: None.

Low	Moderate	High
SC-19	SC-19	SC-19

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST SP 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer resource records.

Low	Moderate	High
Not Selected	SC-20	SC-20

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

Supplemental Guidance: A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST SP 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.

Enhancement *Supplemental Guidance*: Local clients include, for example, DNS stub resolvers.

Low	Moderate	High
Not Selected	Not Selected	SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative DNS servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility).

If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides

name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified. NIST SP 800-81 provides guidance on secure DNS deployment.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SC-22	SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST SP 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST SP 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST SP 800-95 provides guidance on secure web services.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SC-23	SC-23

18. **SYSTEM AND INFORMATION INTEGRITY CONTROLS**. Integrity controls protect data in an information system from accidental or malicious alteration or destruction and provide assurance to the user that the information meets criteria about its quality and reliability.

Table 18. System and Information Integrity Controls

System and Information Integrity				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2 (3)	SI-2 (2)(3)	SI-2 (1)(2)(3)

System and Information Integrity				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SI-3	Malicious Code Protection	SI-3	SI-3 (1)(2)	SI-3 (1)(2)
SI-4	Information System Monitoring Tools and Techniques	SI-4	SI-4 (4)	SI-4 (2)(4)(5)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	SI-6	SI-6	SI-6 (1)(2)
SI-7	Software and Information Integrity	Not Selected	SI-7	SI-7 (1)(2)
SI-8	Spam Protection	SI-8	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Input Accuracy, Completeness, and Validity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance. NIST SP 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

Low	Moderate	High
SI-1	SI-1	SI-1

SI-2 FLAW REMEDIATION

Control: The organization identifies, reports, and corrects information system flaws.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. NIST SP 800-40 provides guidance on security patch installation and patch management.

Related Security Controls: CA-2, CA-4, CA-7, CM-3, IR-4, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs updates automatically.

(2) The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.

(3) **The organization defines and employs metrics for determining the effectiveness of the patch and vulnerability management processes.**

Low	Moderate	High
SI-2 (3)	SI-2 (2)(3)	SI-2 (1)(2)(3)

SI-3 MALICIOUS CODE PROTECTION

Control: The information system implements malicious code protection.

Supplemental Guidance: The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported:

- by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means or

- by exploiting information system vulnerabilities.

The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST SP 800-83 provides guidance on implementing malicious code protection.

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates malicious code protection mechanisms.

Low	Moderate	High
SI-3	SI-3 (1)(2)	SI-3 (1)(2)

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Supplemental Guidance: Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software).

Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the

organization based upon its monitoring objectives and the capability of the information system to support such activities.

Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST SP 800-61 provides guidance on detecting attacks through various types of security technologies. NIST SP 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST SP 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST SP 800-94 provides guidance on intrusion detection and prevention.

Related Security Control: AC-8.

Control Enhancements:

(1) The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

(2) The organization employs automated tools to support near-real-time analysis of events.

(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Enhancement Supplemental Guidance:

Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.

(5) The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].

Low	Moderate	High
SI-4	SI-4 (4)	SI-4 (2)(4)(5)

SI-5 SECURITY ALERTS AND ADVISORIES

Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

Supplemental Guidance: The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that:

- facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies);
- provide access to advice from security professionals; and
- improve knowledge of security best practices. NIST SP 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Control Enhancements:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

Low	Moderate	High
SI-5	SI-5	SI-5 (1)

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system verifies the correct operation of security functions [*Selection (one or more): either upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period,* ***at least annually***] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Control Enhancements:

(1) The organization employs automated mechanisms to provide notification of failed automated security tests.

(2) The organization employs automated mechanisms to support management of distributed security testing.

Low	Moderate	High
SI-6	SI-6	SI-6 (1)(2)

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The information system detects and protects against unauthorized changes to software and information.

Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Control Enhancements:

(1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the system.

(2) The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.

(3) The organization employs centrally managed integrity verification tools.

Low	Moderate	High
Not Selected	SI-7	SI-7 (1)(2)

SI-8 SPAM PROTECTION

Control: The information system implements spam protection.

Supplemental Guidance: The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple

vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST SP 800-45 provides guidance on electronic mail security.

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The information system automatically updates spam protection mechanisms.

Low	Moderate	High
SI-8	SI-8	SI-8 (1)

SI-9 INFORMATION INPUT RESTRICTIONS

Control: The organization restricts the capability to input information to the information system to authorized personnel.

Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SI-9	SI-9

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY

Control: The information system checks information for accuracy, completeness, validity, and authenticity.

Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SI-10	SI-10

SI-11 ERROR HANDLING

Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.

Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SI-11	SI-11

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains output from the information system in accordance with applicable laws, Executive orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: None.

Control Enhancements: None.

Low	Moderate	High
Not Selected	SI-12	SI-12

19. **PROTECTION OF SENSITIVE UNCLASSIFIED INFORMATION INCLUDING PERSONALLY IDENTIFIABLE INFORMATION**. Sensitive unclassified information and Personally Identifiable Information controls to ensure adequate protection of sensitive unclassified information (SUI), including personally identifiable information (PII), associated with all information systems operated by the Department

and its contactors. These controls apply requirements and guidance from Office of Management and Budget (OMB) Memorandum (M) 06 -16, *Protection of Sensitive Agency Information*, the sections of OMB M 06 -19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, and OMB M 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Attachment 1, pertaining to the protection of PII. Processes and criteria for privacy impact assessments are outside the scope of this document.

Table 19. SUI/PII Controls**SUI/PII Controls**				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
E-SU-1	SUI/PII Policy and Procedures	E-SU-1 (1)(2)	E-SU-1 (1)(2)	E-SU-1 (1)(2)
E-SU-2	Use of Encryption	E-SU-2 (1)(2)	E-SU-2 (1)(2)	E-SU-2 (1)(2)
E-SU-3	Remote Access to SUI/PII	E-SU-3 (1)(2)	E-SU-3 (1)(2)	E-SU-3 (1)(2)
E-SU-4	Management of PII on Portable/Mobile Devices and Removable Media	E-SU-4 (1)(2)(3)	E-SU-4 (1)(2)(3)	E-SU-4 (1)(2)(3)

E-SU-1 SUI/PII POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and
- formal, documented procedures to facilitate the implementation of the SUI/PII policy and associated controls.

Supplemental Guidance: The default condition is that P2P applications, technology, or services are not be used on DOE systems that contain or process Sensitive Unclassified Information (SUI), including PII. If the application of P2P technology or service is required, each application of the technology is justified to and approved by the DAA during the Initiation Phase of C&A.

SUI is defined below; Senior DOE Management can extend the definition of SUI to include other types of sensitive information that they determine require this level of protection within their organizations. Extensions of the definition of SUI must be documented in the PCSP. PII is defined in the requirements documented by the Senior Agency Official for Privacy.

- **Sensitive Unclassified Information.** Unclassified information requiring protection mandated by policy or laws, such as Official Use Only (OUO), Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), unclassified Naval Nuclear Propulsion Information (NNPI), Personally Identifiable Information, and other information specifically designated as requiring SUI protection (e.g., sensitive unclassified Cooperative Research and Development Agreements (CRADA) information, etc.)

Control Enhancements:

(1) Protection requirements, control procedures, identification of SUI/PII, and use of encryption software for SUI/PII are included in user training for SUI/PII users.

(2) Awareness training includes the identification of SUI/PII.

Low	Moderate	High
E-SU-1 (1)(2)	E-SU-1 (1)(2)	E-SU-1 (1)(2)

E-SU-2 USE OF ENCRYPTION

Control: FIPS 140-2 Level 1 or higher encryption is implemented for protection of all SUI on all portable/mobile devices and removable media, such as CDROMs or thumb drives containing SUI/PII must be encrypted.

Supplemental Guidance: Agencies may retain and use FIPS 140-1 validated products that have been purchased before the end of the transition period (November 25, 2001). After the transition period, modules will no longer be tested against the FIPS 140-1 requirements. After the transition period, all previous validations against FIPS 140-1 will still be recognized. See http://csrc.nist.gov/publications/fips/). The URL for the Cryptographic Module Validation Program is http://csrc.nist.gov/groups/STM/cmvp/index.html. The FIPS 140-2 standard also acknowledges the use of cryptography approved by the National Security Agency as an appropriate alternative. Consult FIPS 140-2 for specific guidance.

Control Enhancements:

(1) FIPS 140-2 Level 1 or higher encryption is applied during the transmission of all SUI/PII unless communications media can provide an equivalent protection as determined by the DAA. NIST-certified FIPS 140-1 encryption may continue be used. Encryption of SUI/PII in storage is not required until the file has been removed from storage and returned to use.

(2) Decryption capabilities or recovery of encryption keys are available, on request, to law enforcement officials, cyber incident management personnel, and cyber forensics personnel.

Low	Moderate	High
E-SU-2 (1)(2)	E-SU-2 (1)(2)	E-SU-2 (1)(2)

E-SU-3 REMOTE ACCESS TO SUI/PII

Control: Security controls are implemented on all remote access to SUI/PII.

Control Enhancements:

(1) At least two-factor authentication is used for all remote access to SUI/PII.

(2) A user activity time-out function, of at least a minimum of 30 minutes of inactivity, is in place on all information systems supporting remote access to SUI/PII. User re-authentication is required after an inactivity timeout.

Low	Moderate	High
E-SU-3 (1)(2)	E-SU-3 (1)(2)	E-SU-3 (1)(2)

E-SU-4 MANAGEMENT OF PII ON PORTABLE/MOBILE DEVICES AND REMOVABLE MEDIA

Control: PII on Portable/Mobile Devices and Removable Media is managed. All portable/mobile devices are assumed to contain PII unless the DAA determines there is no PII on the device, in writing.

Supplemental Guidance: Written approval of the SSP will constitute the written determination of no PII on the device.

Related Security Controls: RA-2.

Control Enhancements:

(1) Procedures for periodic review of all portable/mobile devices and removable media for PII are established, documented and implemented.

(2) Procedures for removal of files containing PII that are 90 days or older are established, documented, and implemented.

(3) Approval for use of files containing PII on portable/mobile devices and removable media for longer than the 90-day period must be documented in the SSP[8].

Low	Moderate	High
E-SU-4(1)(2)(3)	E-SU-4(1)(2)(3)	E-SU-4(1)(2)(3)

[8] Owners of portable/mobile devices and removable media and their supervisors should be involved in the review of the content of their devices that they use, since they are most familiar with such content. The review must be thoroughly and accurately documented to provide sufficient information to properly determine the disposition of the content of each device.

CONTRACTOR REQUIREMENTS DOCUMENT
DOE M 205.1-7, *Security Controls For Unclassified Systems 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.

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

ADMIN CHANGE

DOE M 205.1-7 Chg 1

Approved: 1-5-09
Admin Chg 1: 9-1-09

SUBJECT: SECURITY CONTROLS FOR UNCLASSIFIED INFORMATION SYSTEMS MANUAL

1. PURPOSE. To transmit the revised page to DOE M 205.1-7, *Security Controls for Unclassified Information Systems Manual,* dated 1-5-09.

2. EXPLANATION OF CHANGES. This change amends the date for Senior DOE Management Program Security Plans to require their operating units to implement and maintain at least the minimum requirements of the Manual for information systems operated by or on behalf of the Department.

3. LOCATION OF CHANGE.

Page	Paragraph
ii	4.c.

After filing the attached pages, this transmittal may be discarded.

BY ORDER OF THE SECRETARY OF ENERGY:

KEVIN T. HAGERTY
Director
Office of Information Resources
Office of Management