

**U.S. Department of Energy
Cyber Security Program**

**Management, Operational, and
Technical Controls
Guidance**



July 6, 2006

Table of Contents

- 1. PURPOSE1
- 2. CANCELLATIONS.....1
- 3. APPLICABILITY.....1
- 4. IMPLEMENTATION.....2
- 5. MANAGING ORGANIZATIONAL RISK.....2
- 6. STRUCTURE OF CONTROLS FOR UNCLASSIFIED INFORMATION SYSTEMS.4
- 7. SECURITY CATEGORY AND BASELINES.4
- 8. ACCESS CONTROL.....8
- 9. AWARENESS AND TRAINING.....13
- 10. AUDIT AND ACCOUNTABILITY.16
- 11. CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT CONTROLS.....19
- 12. CONFIGURATION MANAGEMENT.21
- 13. CONTINGENCY PLANNING.23
- 14. IDENTIFICATION AND AUTHENTICATION.....27
- 15. INCIDENT RESPONSE.....30
- 16. MAINTENANCE.32
- 17. MEDIA PROTECTION.34
- 18. PHYSICAL AND ENVIRONMENTAL PROTECTION.....36
- 19. PLANNING CONTROLS.41
- 20. PERSONNEL SECURITY.....42
- 21. RISK ASSESSMENT.....45
- 22. SYSTEM AND SERVICES ACQUISITION.....47
- 23. SYSTEM AND COMMUNICATIONS PROTECTION.50
- 24. SYSTEM AND INFORMATION INTEGRITY.....54
- 25. REFERENCES.....57
- 26. DEFINITIONS.58
- 27. CONTACT.....58
- ATTACHMENT 1.....59
- PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-1 IS APPLICABLE59
- ATTACHMENT 2 REFERENCES60
- ATTACHMENT 3 ACRONYMS.....63
- ATTACHMENT 4 GLOSSARY64

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance implements National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication (PUB) FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*; NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, and the DOE cyber security program criteria for the implementation of management, operations, and technical controls for unclassified information systems within the DOE, including the National Nuclear Security Administration (NNSA).

The DOE CIO will review this guidance annually and update it as necessary. Senior DOE Management, and their operating units, may provide feedback at any time for incorporation into the next scheduled update.

2. CANCELLATIONS.

None.

3. APPLICABILITY.

- a. Primary DOE Organizations. This guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to which DOE CIO Guidance CS-1 is Applicable*.

Further, the DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats not previously addressed, or created in respect to the DOE and alignment between their subordinate organizations and contractors (hereinafter called operating units), and for ensuring that those requirements are incorporated into contracts.

- b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Order for activities under the NNSA Deputy Administrator's cognizance.
- c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.

- d. National Security Systems. This guidance is not mandatory, but may be used with DOE national security systems. Senior DOE Management Program Cyber Security Plans (PCSPs) are to address the criteria outlined in DOE CIO Guidance CS-22, *National Security Systems Controls*, for all DOE National Security information systems. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides guidance for identifying national security systems.

4. IMPLEMENTATION.

This guidance is effective 30 days after issuance. However, DOE recognizes that this guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its effective date. If Senior DOE Management cannot address all of the criteria by the scheduled milestone, DOE expects Senior DOE Management to establish a Plan of Actions and Milestones for implementation of this Guidance into the PCSP.

5. MANAGING ORGANIZATIONAL RISK.

The selection and specification of security controls for an information system is accomplished as part of a Department-wide information security program that involves the management of organizational risk—that is, the risk associated with the operation of an information system. The management of organizational risk is a key element in the Department’s information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect the operations and assets of the organization.

Managing organizational risk includes several important activities: (i) assessing risk; (ii) conducting cost-benefit analyses; (iii) selecting, implementing, and assessing security controls; and (iv) formally authorizing the information system for operation (also known as security accreditation). The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, Directives, Executive Orders, policies, standards, or regulations. Each Senior DOE Management organization is to document its approach to managing organizational risk through the organization’s PCSP.

In addition, Senior DOE Management are to develop and issue to each operating unit through their PCSPs, mission-oriented implementation policies for the criteria in this Guidance. The PCSP is to describe the risk management or mission impact rationale for all criteria not fully addressed in the implementation policies.

The following activities related to managing organizational risk in the Senior DOE Management organization and its operating units are paramount to an effective information security program and can be applied through the Senior DOE Management PCSP to both new and legacy information systems within the context of the System Development Life Cycle and the DOE Enterprise Architecture—

- **Categorize** information systems and the information resident within the system based on an impact analysis using FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- **Select** an initial set of security controls (i.e., baseline) from the Senior DOE Management PCSP for the information system as a starting point for the risk assessment process based on the FIPS 199 security categorization.
- **Adjust** (or tailor) the initial set of security controls based on an assessment of risk and local conditions including Senior DOE Management or site-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or special circumstances.
- **Document** the set of security controls in the System Security Plan (SSP) for the information system including the operating unit's justification for any refinements or adjustments to the initial set of controls.
- **Implement** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.
- **Assess** the security controls using appropriate methods and procedures 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.
- **Determine** the risk to organizational DOE operations and assets resulting from the planned or continued operation of the information system.
- **Authorize** information system processing (or for legacy systems, authorize continued system processing) if the level of risk to the organization's operations or assets is acceptable.
- **Monitor and assess** selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

Senior DOE Management PCSPs are to require that operating units comply with this Guidance criteria in developing an acceptable control baseline for each unclassified information system appropriate to the impact level of the system. NIST SP 800-53 identifies the following control Classes, Families, and Identifiers as shown in **Table 1**. To uniquely identify each control, a numeric identifier is appended to the Family identifier to indicate that control within the Family. For example, RA-1 represents control number 1 within the Risk Assessment Family.

Table 1. Cyber Security Control Classes, Families and Identifiers

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL

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

6. STRUCTURE OF CONTROLS FOR UNCLASSIFIED INFORMATION SYSTEMS.

This Guidance defines DOE, including NNSA, criteria (denoted by the terms “are to,” “must,” “will,” and “require”) and recommended (denoted by the terms “should” and “may”) controls for unclassified information systems.

Supplemental issue-specific Guidance provides more detail on criteria and includes the processes to be followed in implementing the criteria outlined in this guidance within DOE, including NNSA. For example, DOE OCIO Guidance CS-2, *Cyber Security Program Certification and Accreditation Guidance*, provides guidance on expected and recommended practices for effectively performing the certification and accreditation of Departmental unclassified information systems.

Senior DOE Management PCSPs may supplement the criteria in this, and associated issue-specific, guidance with additional and/or more stringent requirements based on the unique computing environment. The DOE criteria for these security controls are based on the recommendations of the NIST SP 800-53. The criteria are described by security control baseline (i.e., low, moderate, and high). Using a format similar to security controls, some criteria are augmented by supplemental guidance that provides additional detail and explanation of how the criteria are to be addressed.

7. SECURITY CATEGORY AND BASELINES.

NIST SP 800-53 notes that the security controls applied to a particular information system should be commensurate with the potential impact on organizational operations, organizational assets, or individuals should there be a breach in security due to the loss of data or system confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information resident on the information systems. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume I and Volume II, provides guidance on the assignment of security categories to information systems. The generalized format for expressing the security category of an *information system* is:

Information system security category = {(confidentiality, **impact**), (integrity, **impact**),
(availability, **impact**)},

Where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not be identical for an information system, the high water mark concept is used to determine the impact level of the information system and select an initial set of security controls from the three defined in NIST SP 800-53. Thus, a *low-impact* system is defined as an information system in which all three of the security objectives are low. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact* system is an information system in which at least one security objective is high. Once the overall impact level of the information system is determined, an initial set of security controls can be selected from the minimum controls in this Guidance as described below.

a. Low Baseline

Assurance Level: The security control is in effect and meets explicitly identified functional criteria in the control statement.

Supplemental Guidance: For security controls in the low baseline, the focus is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

b. Moderate Baseline

Assurance Level: The security control is in effect and meets explicitly identified functional criteria in the control statement. The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in the moderate baseline, the focus is on ensuring correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation to ensure the control meets its required function or purpose.

c. High Baseline

Assurance Level: The security control is in effect and meets explicitly identified functional criteria in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control (including functional interfaces among control components). The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in the high baseline, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. For security controls in the high baseline, this same documentation is needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

d. Additional Criteria Enhancing the Moderate and High Baselines

Assurance Requirement: The security control is in effect and meets explicitly identified functional criteria in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions to ensure that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.

e. DOE Control Guidance

NIST SP 800-53 allows for changes and refinements of security controls by an Agency. DOE has made two types of changes and refinements.

- (1) DOE changes to a control baseline are highlighted in the control family tables by gray shading, and the changes are explained in the accompanying control text.
- (2) DOE specifications of a control parameter or refinement of a control are enclosed in brackets (‘[‘), and the text is italicized and in bold font.

Each statement of management, operation, or technical control where DOE security control guidance has been identified contains a reference identifying where the DOE criteria for the control are documented.

f. Common Security Controls

A Senior DOE Management organization-wide view of an information security program facilitates the identification of *common security controls* that can be applied to one or more program or sites within the organization. Common security controls can apply to: (i) all organizational information systems; (ii) a group or enclave of information systems at a specific site; or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of organizational information systems where the controls have been applied.

The identification of common security controls is most effectively accomplished with the involvement of the Senior DOE Management organization’s Chief Information Officer (or equivalent), cyber security point of contact, designated approving authorities, information system owners/program managers, and information system security officers. For example, a Senior DOE Management PCSP could identify and require certain common security controls for all low-impact information systems in the organization by considering the baseline security controls for that category of information system. Similar exercises can be conducted for moderate-impact and high-impact systems as well.

Many of the security controls needed to protect an information system or enclave (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) may be excellent candidates for common security control status. By centrally managing the development, implementation, and assessment of the common security controls designated by the Senior DOE Management organization, security costs can be amortized across multiple information systems. Careful management of the selection and implementation of common controls is needed because the potential dependence on common security controls by many of an organization’s information systems may result in a significant increase in organization-level risk in the event of a failure of the controls.

Partitioning security controls into common security controls and system-specific security controls can result in significant savings to the organization in control development and implementation costs. It can also result in a more consistent application of the security controls across the organization at large. Moreover, equally significant savings can be realized in the security certification and accreditation process. Rather than assessing

common security controls in every information system, the certification process can draw upon the results from the most current assessment of the common security controls. The Senior DOE Management organization-wide approach to reuse and sharing of assessment results can greatly enhance the efficiency of the security certification and accreditation process, improve the quality of the certification and accreditation process, and significantly reduce security program costs.

8. ACCESS CONTROL.

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. In the PCSP, Senior DOE Management are to address the access control controls listed in Table 2 for all general support systems and major applications under their responsibility.

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)	AC-2 (1) (2)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Applicable	AC-4	AC-4
AC-5	Separation of Duties	Not Applicable	AC-5	AC-5
AC-6	Least Privilege	Not Applicable	AC-6	AC-6
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7 (1)	AC-7 (1)
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Applicable	Not Applicable	Not Applicable
AC-10	Concurrent Session Control	Not Applicable	Not Applicable	AC-10
AC-11	Session Lock	Not Applicable	AC-11	AC-11
AC-12	Session Termination	Not Applicable	AC-12	AC-12
AC-13	Supervision and Review—Access Control	AC-13	AC-13	AC-13 (1)
AC-14	Permitted Actions w/o Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Applicable	Not Applicable	AC-15
AC-16	Automated Labeling	Not Applicable	Not Applicable	Not Applicable
AC-17	Remote Access	AC-17	AC-17 (1)	AC-17 (1)
AC-18	Wireless Access Restrictions	Not Applicable	AC-18 (1)	AC-18 (1)

Access Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
AC-19	Access Control for Portable and Mobile Devices	Not Applicable	AC-19	AC-19 (1)
AC-20	Personally Owned Information Systems	AC-20	AC-20	AC-20

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, security assessment and access control policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access controls for all information systems in all Senior DOE Management operating units.

AC-2 ACCOUNT MANAGEMENT

Manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts and document the procedures for managing the accounts.

(1) For MODERATE- and HIGH-impact systems:

- Employ automated mechanisms to support the management of information system accounts.
- Automatically terminate temporary and emergency accounts after a reasonable period as specified by the Senior DOE Management PCSP.
- Automatically disable inactive accounts after reasonable period as specified by the Senior DOE Management PCSP.

(2) Employ automated mechanisms for HIGH-impact information systems account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.

AC-3 ACCESS ENFORCEMENT

Enforce assigned authorizations for controlling access to the information system in accordance with applicable policy.

(1) For MODERATE and HIGH-impact systems, access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).

AC-4 INFORMATION FLOW ENFORCEMENT

For MODERATE- and HIGH-impact information systems, enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

AC-5 SEPARATION OF DUTIES

For MODERATE- and HIGH-impact information systems, enforce separation of duties through assigned access authorizations.

AC-6 LEAST PRIVILEGE

For MODERATE- and HIGH-impact information systems, enforce 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.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Document in information system SSPs and enforce a limit of [*PCSP specified number*] consecutive invalid access attempts by a user during a [*operating unit specified*] time period. The information system automatically [*locks the account/node for a time period defined by the operating unit or delays next login prompt according to a specified algorithm*] when the maximum number of unsuccessful attempts is exceeded.

- (1) For HIGH-impact systems, automatically lock the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

AC-8 SYSTEM USE NOTIFICATION

Display an approved system-use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) 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.

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**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**WARNING****

AC-9 PREVIOUS LOGON NOTIFICATION

Control AC-9 is not required at this time. Senior DOE Management PCSPs may specify or operating units, may elect, at their discretion, to ensure that information systems notify the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

AC-10 CONCURRENT SESSION CONTROL

For HIGH-impact information systems, limit the number of concurrent sessions for any user [*as defined in the information system SSP*].

AC-11 SESSION LOCK

For MODERATE- and HIGH-impact information systems, prevent further access to the information system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

AC-12 SESSION TERMINATION

For MODERATE- and HIGH-impact information systems, automatically terminate a session after [*a period of inactivity specified in the information system SSP*].

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Supervise and review the activities of users with respect to the enforcement and usage of information system access controls.

- (1) Employ automated mechanisms to facilitate the review of user activities for HIGH-impact information systems.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Identify specific user actions that can be performed on the information system without identification or authentication.

- (1) For MODERATE- and HIGH-impact information systems, permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

AC-15 AUTOMATED MARKING

For HIGH-impact information systems, mark output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

AC-16 AUTOMATED LABELING

Control AC-16 is not required, at this time. Senior DOE Management PCSPs may specify or operating units, may elect, at their discretion, to ensure that information in storage, in process, or in transmission is appropriately labeled by an information system.

AC-17 REMOTE ACCESS

Document, monitor, and control all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

- (1) For MODERATE and HIGH-impact systems:
 - Employ automated mechanisms to facilitate the monitoring and control of remote access methods.
 - Use encryption to protect the confidentiality of remote access sessions.
 - Control all remote accesses through a managed access control point.

NOTE: DOE CIO Guidance CS-24, *Remote Access to DOE Information Systems*, describes criteria for remote access to information systems in DOE.

AC-18 WIRELESS ACCESS RESTRICTIONS

Establish usage restrictions and implementation guidance for wireless technologies; and document, monitor, and control wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.

- (1) Use authentication and encryption to protect wireless access to MODERATE and HIGH-impact systems

NOTE: DOE CIO Guidance CS-13, *Wireless Devices and Information Systems*, describes criteria for using wireless devices and information systems within DOE.

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Establish usage restrictions and implementation guidance for portable and mobile devices; and document, monitor, and control device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.

- (1) Employ removable hard drives or cryptography to protect information residing on MODERATE and HIGH-impact system portable and mobile devices.

NOTE: DOE CIO Guidance CS-14, *Portable and Mobile Devices*, describes criteria for using portable and mobile devices and information systems within DOE.

AC-20 PERSONALLY OWNED INFORMATION SYSTEMS

Restrict the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of Federal information.

NOTE: DOE CIO Guidance CS-15, *Personally Owned Information Systems*, describes criteria for using personally owned devices and information systems within DOE.

9. AWARENESS AND TRAINING.

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. Awareness activities provide the means to focus attention on cyber security. Awareness presentations allow individuals to recognize cyber security concerns and respond accordingly. 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. Senior DOE Management PCSPs are to address the awareness and training controls listed in **Table 3**.

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-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, awareness and training policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-31, *Awareness and Training*, describes the DOE criteria for awareness and training controls.

AT-2 SECURITY AWARENESS

Provide all users (including managers and senior executives) with basic cyber security awareness instruction [*within 30 days of appointment*] and before authorizing permanent access to a system, and [*at least annually*] thereafter. This instruction must present a core set of generic cyber security terms and concepts for all personnel (Federal employees and contractors) as a baseline for role-based learning, expands on those basic concepts, and provides a mechanism for students to relate and apply the information learned on the job.

AT-3 SECURITY TRAINING

Identify personnel with significant cyber security roles and responsibilities, document those roles and responsibilities, and provide appropriate cyber security training before authorizing access to the system. Establish [*and, at least bi-annually, execute*] training plans for these personnel covering the training topics described in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*.

NOTE: DOE CIO Guidance CS-31, *Awareness and Training*, describes criteria for education and training within DOE

AT-4 SECURITY TRAINING RECORDS

Document and monitor individual cyber security training activities, including basic security awareness training and specific cyber security training.

10. AUDIT AND ACCOUNTABILITY.

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, and opening a file. In their PCSPs, Senior DOE Management are to address the audit and accountability controls listed in **Table 4** for all general support systems and major applications under their responsibility.

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	AU-2 (1)
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	Audit Processing	AU-5	AU-5	AU-5 (1)
AU-6	Audit Monitoring, Analysis, and Reporting	AU-6	AU-6	AU-6 (1)
AU-7	Audit Reduction and Report Generation	AU-7	AU-7	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8	AU-8
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Applicable	Not Applicable	Not Applicable
AU-11	Audit Retention	AU-11	AU-11	AU-11

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, audit and accountability policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-34, *Audit and Accountability Controls*, describes the DOE criteria for audit and accountability controls.

AU-2 AUDITABLE EVENTS

[Document in the information system SSPs what events generate audit records for their information systems].

(1) For HIGH-impact information systems:

- Compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.
- Manage the selection of events to be audited by individual components of the system.

AU-3 CONTENT OF AUDIT RECORDS

Capture sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.

- (1) For MODERATE and HIGH-impact information systems, provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
- (2) For HIGH-impact information systems, provide the capability to centrally manage the content of audit records generated by individual components throughout the system.

AU-4 AUDIT STORAGE CAPACITY

Allocate sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

AU-5 AUDIT PROCESSING

In the event of an audit failure or audit storage capacity being reached, alert appropriate organizational officials and take the additional actions [*specified by the information system SSP- (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)*].

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Regularly review/analyze audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

- (1) Employ automated mechanisms for HIGH-impact information systems to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Employ automated mechanisms for HIGH-impact information systems to immediately alert security personnel of inappropriate or unusual activities with security implications.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Provide an audit reduction and report generation capability for each information system.

- (1) For HIGH-impact information systems, provide the capability to automatically process audit records for events of interest based upon selectable, event criteria.

AU-8 TIME STAMPS

For MODERATE- and HIGH-impact systems, provide time stamps for use in audit record generation.

AU-9 PROTECTION OF AUDIT INFORMATION

Protect system audit information and audit tools from unauthorized access, modification, and deletion.

AU-10 NON-REPUDIATION

Control AU-10 is not required, at this time. Senior DOE Management PCSPs may specify or operating units, may elect, at their discretion, to ensure that information systems provide the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information e.g., to indicate concurrence or sign a contract or received a message).

AU-11 AUDIT RETENTION

Retain audit logs for [*a time period specified in information system SSP and as consistent with Departmental and National Archives and Records Administration retention periods*], to provide support for after-the-fact investigations of security incidents and meet regulatory and organizational information retention requirements.

11. CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT 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. In their PCSPs, Senior DOE Management are to address the C&A and security assessment controls listed in **Table 5** for all general support systems and major applications under their responsibility.

Table 5. Certification, Accreditation, and Security Assessment Controls

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

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

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, security assessment and certification and accreditation policies, practices, and processes

that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies, practices, and processes and associated assessment, certification, and accreditation controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-2, *Certification and Accreditation Process for Information Systems, Including National Security Systems*, describes the criteria for certification and accreditation of all information systems within DOE.

CA-2 SECURITY ASSESSMENTS

Conduct assessments of the effectiveness of security controls in each information system [*at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome in meeting the security requirements for the system.

CA-3 INFORMATION SYSTEM CONNECTIONS

Explicitly authorize all connections to an information system from outside of the accreditation boundary be and monitor/control the system interconnections on an ongoing basis.

NOTE: DOE CIO Guidance CS-5, *Interconnection Agreements*, describes the DOE criteria for interconnection of information systems within DOE

CA-4 SECURITY CERTIFICATION

Perform an assessment of 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.

CA-5 PLAN OF ACTION AND MILESTONES

Develop and update [*according to the frequency specified in the PCSP*], a plan of action and milestones (POA&M) for its information systems that documents the operating unit's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

NOTE: DOE CIO Guidance CS-6, *POA&M Guidance*, describes the criteria for developing and maintaining POA&Ms for all information systems within DOE.

CA-6 SECURITY ACCREDITATION

Authorize (i.e., accreditation) each information system for processing before operations and update the authorization [*at least every 3 years or upon significant change to the system*].

CA-7 CONTINUOUS MONITORING

Continuously monitor the effectiveness and adequacy of system controls in accordance with the Senior DOE Management PCSP.

12. CONFIGURATION MANAGEMENT.

In their PCSPs, Senior DOE Management are to address the configuration management controls listed in Table 6 for all general support systems and major applications under their responsibility,

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	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	Not Applicable	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Applicable	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Applicable	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Applicable	CM-7	CM-7 (1)

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, configuration management policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-8, *Configuration Management*, describes the criteria for configuration management for all information systems within DOE.

CM-2 BASELINE CONFIGURATION

Develop, document, and maintain a current baseline configuration of the information system and an inventory of the system's constituent components.

- (1) Update baseline configurations for MODERATE- and HIGH-impact information systems as an integral part of information system component installations.
- (2) Employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration for HIGH-impact information systems.

CM-3 CONFIGURATION CHANGE CONTROL

Document and control changes to MODERATE- and HIGH-impact information systems. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.

- (1) Employ automated mechanisms for HIGH-impact information systems to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

CM-4 MONITORING CONFIGURATION CHANGES

Monitor changes to MODERATE- and HIGH-impact information systems and conduct security impact analyses to determine the effects of the changes.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Enforce access restrictions associated with changes to MODERATE- and HIGH-impact information systems.

- (1) Employ automated mechanisms for HIGH-impact information systems to enforce access restrictions and support auditing of the enforcement actions.

CM-6 CONFIGURATION SETTINGS

Configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.

- (1) Employ automated mechanisms for HIGH-impact information systems to centrally manage, apply, and verify configuration settings.

CM-7 LEAST FUNCTIONALITY

Configure MODERATE- and HIGH-impact information systems to provide only essential capabilities [*and document in system security plans specific prohibitions and/or restrictions upon the use of functions, ports, protocols, and/or services*].

- (1) Review HIGH-impact information systems the information system [*at least annually*], to identify and eliminate unnecessary functions, ports, protocols, and/or services.

13. CONTINGENCY PLANNING.

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.

In their PCSPs, Senior DOE Management are to address the contingency planning controls listed in Table 7 for all general support systems and major applications under their responsibility.

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)
CP-3	Contingency Training	Not Applicable	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	Not Applicable	CP-4	CP-4 (1)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Sites	Not Applicable	CP-6 (1)	CP-6 (1) (2)
CP-7	Alternate Processing Sites	Not Applicable	CP-7	CP-7 (1)
CP-8	Telecommunications Services	Not Applicable	CP-8	CP-8
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, contingency

planning policies that address purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated contingency planning policy and associated contingency planning controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-7, *Contingency Planning*, describes the criteria for contingency planning for all information systems within DOE.

CP-2 CONTINGENCY PLAN

Develop and implement a contingency plan for each 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.

- (1) Coordinate contingency plan development with organizational operating units responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan) for MODERATE- and HIGH-impact information systems.

CP-3 CONTINGENCY TRAINING

Train personnel in their contingency roles and responsibilities with respect to MODERATE- and HIGH-impact information systems and provide refresher training [*at least annually*].

- (1) Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations for HIGH-impact information systems.

Use of automated mechanisms is recommended to provide a more thorough and realistic training environment.

CP-4 CONTINGENCY PLAN TESTING

Test the contingency plan for MODERATE- and HIGH-impact information systems [*at least annually*] using [*operating unit-defined tests and exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the operating units review the contingency plan test results and initiate corrective actions.

- (1) Coordinate contingency plan testing for MODERATE- and HIGH-impact information systems with organizational operating units responsible for

related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

- (2) Test the contingency plan for HIGH-impact information systems 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.

For HIGH-impact information systems, the use of automated mechanisms to more thoroughly and effectively test the contingency plan is recommended.

CP-5 CONTINGENCY PLAN UPDATE

Review the contingency plan for the information system [*at least annually*] and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

CP-6 ALTERNATE STORAGE SITES

Identify an alternate storage site and initiate necessary agreements to permit the storage of MODERATE- and HIGH-impact information systems backup information.

For MODERATE- and HIGH-impact information systems, geographically separate alternate storage site(s) from the primary storage site so as not to be susceptible to the same hazards.

- (1) For HIGH-impact information systems, configure alternate storage site(s) to facilitate timely and effective recovery operations and the operating units identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-7 ALTERNATE PROCESSING SITES

Identify an alternate processing site and initiate necessary agreements to permit the resumption of MODERATE- and HIGH-impact information systems operations for critical mission/business functions [*in a timely manner, as specified by the operating units in the information system SSP,*] when the primary processing capabilities are unavailable.

- (1) For MODERATE- and HIGH-impact information systems:
 - Geographically separate Alternate processing site(s) are from the primary processing site so as not to be susceptible to the same hazards;

- Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions; and
 - Include priority-of-service provisions in alternate processing site agreements in accordance with the organization's availability requirements.
- (2) For HIGH-impact information systems, configure alternate processing site(s) to fully support a minimum required operational capability and be ready to use as the operational site.

CP-8 TELECOMMUNICATIONS SERVICES

Identify primary and alternate telecommunications services to support MODERATE- and HIGH-impact information systems and initiate necessary agreements to permit the resumption of MODERATE- and HIGH-impact information systems operations for critical mission/business functions [*in a timely manner, as specified by the operating unit,*] when the primary telecommunications capabilities are unavailable.

- (1) For MODERATE and HIGH-impact information systems:
- Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.
 - Alternate telecommunications services do not share a single point of failure with primary telecommunications services.
- (2) For HIGH-impact information systems:
- Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.
 - Primary and alternate telecommunications service providers have adequate contingency plans.

CP-9 INFORMATION SYSTEM BACKUP

Conduct backups of user-level and system-level information (including system state information) contained in the information system [*at least annually*] and stores backup information at an appropriately secured location.

- (1) Test backup information for MODERATE- and HIGH-impact information systems [*at least annually*] to ensure media reliability and information integrity.

- (2) For HIGH-impact information systems:
- Selective use of backup information in the restoration of information system functions as part of contingency plan testing.
 - Storing of 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.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

- (1) Include a full recovery and reconstitution of HIGH-impact information systems as part of contingency plan testing.

14. IDENTIFICATION AND AUTHENTICATION.

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 a 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 must implement a method of user identification and authentication. 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. In their PCSPs, Senior DOE Management are to address the identification and authentication controls listed in **Table 8** for all general support systems and major applications under their responsibility.

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	IA-2	IA-2 (1)
IA-3	Device Identification and Authentication	Not Applicable	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5

Identification and Authentication				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
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

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, identification and authentication policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls for all information systems in all Senior DOE Management operating units.

- [All information systems require distinct user IDs that are unique to each user or group for user identification.
- *All information systems require a user authentication mechanism 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. The implementation or technology used should provide access security commensurate with the level of sensitivity assigned to the resource (i.e. information, devices or systems).*
- *All information systems and associated equipment that rely on passwords as the means to authenticate users must implement effective password management in accordance with DOE CIO Guidance CS-12, Password Management.]*

NOTE: DOE CIO Guidance CS-12, *Password Management*, describes the DOE criteria for management of passwords.

NOTE: DOE CIO Guidance CS-32, *Identification and Authentication*, describes the DOE criteria for identification and authentication controls.

IA-2 USER IDENTIFICATION AND AUTHENTICATION

Uniquely identify and authenticate users (or processes acting on behalf of users) on all information systems.

(1) For HIGH-impact information systems, employ multifactor authentication.

NOTE: DOE CIO Guidance CS-12, *Password Management*, describes the DOE criteria for the generation and use of passwords.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

For MODERATE and HIGH-impact information systems, identify and authenticate specific devices before establishing a connection.

IA-4 IDENTIFIER MANAGEMENT

Manage user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after a reasonable period of inactivity as documented by the operating unit in its procedures; and (vi) archiving user identifiers.

IA-5 AUTHENTICATOR MANAGEMENT

Manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation. Electronic authentication methods to provide services to citizens must comply with OMB Memorandum 04-04, *E-Authentication Guidance*, and associated implementation requirements in NIST SP 800-63, *Electronic Authentication Guideline*.

NOTE: DOE CIO Guidance CS-12, *Password Management*, describes the DOE criteria for the generation and use of passwords.

IA-6 AUTHENTICATOR FEEDBACK

Provide feedback from the information system to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.

NOTE: DOE CIO Guidance CS-12, *Password Management*, describes the DOE criteria for the generation and use of passwords.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

For information systems that authenticate using a cryptographic module, employ authentication methods compliant with FIPS 140-2.

15. INCIDENT RESPONSE.

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) and from 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. In their PCSPs, Senior DOE Management are to address the incident response controls listed in Table 9 for all general support systems and major applications under their responsibility.

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	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, incident response policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policies and associated incident response controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-9, *Incident Prevention, Warning, and Response Guidance*, describes criteria for cyber security incidents for all information systems within DOE.

IR-2 INCIDENT RESPONSE TRAINING

Train personnel in their incident response roles and responsibilities and provides refresher training [*at least annually*].

- (1) For HIGH-impact information systems:
 - Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.
 - Employ automated mechanisms to provide a more thorough and realistic training environment.

IR-3 INCIDENT RESPONSE TESTING

Test the incident response capability for information systems [*at least annually using tests and exercises defined by the operating unit in the information system SSPs*] to determine the incident response effectiveness and documents the results.

- (1) Employ automated mechanisms for HIGH-impact information systems to more thoroughly and effectively test the incident response capability.

IR-4 INCIDENT HANDLING

Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

- (1) Employ automated mechanisms for MODERATE- and HIGH-impact information systems to support the incident handling process.

IR-5 INCIDENT MONITORING

Track and document cyber security incidents on an ongoing basis.

- (1) Employ automated mechanisms for HIGH-impact information systems to assist in the tracking of security incidents and in the collection and analysis of incident information.

IR-6 INCIDENT REPORTING

Report incident information promptly to appropriate authorities by the responsible incident response capability.

- (1) Employ automated mechanisms for MODERATE- and HIGH-impact information systems to assist in the reporting of security incidents.

IR-7 INCIDENT RESPONSE ASSISTANCE

Provide an incident support resource (e.g., internal or external incident response capability support) that offers advice and assistance to users of the operating unit's information systems for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

- (1) Employ automated mechanisms for MODERATE- and HIGH-impact information systems to increase the availability of incident response-related information and support.

16. MAINTENANCE.

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. In their PCSPs, Senior DOE Management are to address the maintenance controls listed in Table 10 for all general support systems and major applications under their responsibility.

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 Applicable	MA-3	MA-3 (1)
MA-4	Remote Maintenance	MA-4	MA-4	MA-4 (1)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Applicable	MA-6	MA-6

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, system maintenance policies that address purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, compliance; and (ii) formal, documented procedures to facilitate the implementation of the system maintenance policies and associated system

maintenance controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-29, *Maintenance*, describes the DOE criteria for maintenance controls.

MA-2 PERIODIC MAINTENANCE

Schedule, perform, and document routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or operating unit requirements.

- (1) Maintain a maintenance log for MODERATE- and HIGH-impact information systems that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).
- (2) Employ automated mechanisms to ensure that periodic maintenance for HIGH-impact information systems is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.

MA-3 MAINTENANCE TOOLS

Approve, control, and monitor the use of MODERATE- and HIGH-impact information systems maintenance tools and maintains the tools on an ongoing basis.

- (1) For HIGH-impact information systems:
 - Inspect all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.
 - Check all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.
 - Check all maintenance equipment with the capability of retaining information to ensure 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.
 - Employ automated mechanisms to ensure only authorized personnel use maintenance tools.

MA-4 REMOTE MAINTENANCE

Approve, control, and monitor remotely executed maintenance and diagnostic activities.

(1) For HIGH-impact information systems:

- Audit all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.
- Address the installation and use of remote diagnostic links in the system security plan for the information system.
- Remote diagnostic or maintenance services are acceptable if performed by a service or operating unit that implements for its own information system the same level of security as that implemented on the information system being serviced.

MA-5 MAINTENANCE PERSONNEL

Maintain a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.

MA-6 TIMELY MAINTENANCE

Obtain maintenance support and spare parts for [*key MODERATE- and HIGH-impact information systems components*] within [*a time frame to support mission requirement*] following a failure.

17. MEDIA PROTECTION.

DOE, including NNSA, requires that operating unit cyber security programs include procedures for storing, handling, and destroying national and non-national security information media. In their PCSPs, Senior DOE Management are to address the media protection controls listed in Table 11 for all general support systems and major applications under their responsibility.

Table 11. Media Protection Controls

Media Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2	MP-2 (1)

Media Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
MP-3	Media Labeling	Not Applicable	MP-3	MP-3
MP-4	Media Storage	Not Applicable	MP-4	MP-4
MP-5	Media Transport	Not Applicable	MP-5	MP-5
MP-6	Media Sanitization	MP-6	MP-6	MP-6
MP-7	Media Destruction and Disposal	MP-7	MP-7	MP-7

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, media protection policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policies and associated media protection controls for all information systems in all Senior DOE Management operating units.

MP-2 MEDIA ACCESS

Allow access to information in printed form or on digital media removed from the information system to authorized users only.

- (1) Unless guard stations control access to media storage areas, employ automated mechanisms for HIGH-impact information systems to ensure only authorized access to such storage areas and to audit access attempts and access granted.

MP-3 MEDIA LABELING

Affix external labels to MODERATE- and HIGH-impact information system removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. [*The operating unit must document in the information system SSP the specific types of media or hardware components*] exempt from labeling so long as they remain within a secure environment.

MP-4 MEDIA STORAGE

Physically control and securely store MODERATE- and HIGH-impact information systems media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.

MP-5 MEDIA TRANSPORT

Control MODERATE- and HIGH-impact information system media (paper and electronic) and restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

MP-6 MEDIA SANITIZATION

Sanitize digital media using approved equipment, techniques, and procedures. The operating unit tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.

NOTE: DOE CIO Guidance CS-11, *Clearing, Sanitization, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Guidance*, describes the DOE criteria for media sanitization.

MP-7 MEDIA DESTRUCTION AND DISPOSAL

Sanitize or destroy information system digital media before its disposal or release for reuse outside the organization to prevent unauthorized individuals from gaining access to and using the information contained on the media.

NOTE: DOE CIO Guidance CS-11, *Clearing, Sanitization, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Guidance*, describes the DOE criteria for media destruction and disposal.

18. PHYSICAL AND ENVIRONMENTAL PROTECTION.

In their PCSPs, Senior DOE Management are to address the physical and environmental controls listed in **Table 12** for all general support systems and major applications under their responsibility.

Table 12. Physical and Environmental 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
PE-4	Access Control for Transmission Medium	Not Applicable	Not Applicable	Not Applicable
PE-5	Access Control for Display Medium	Not Applicable	PE-5	PE-5

Physical and Environmental Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Logs	PE-8	PE-8 (1)	PE-8 (1)
PE-9	Power Equipment and Power Cabling	Not Applicable	PE-9	PE-9
PE-10	Emergency Shutoff	Not Applicable	PE-10	PE-10
PE-11	Emergency Power	Not Applicable	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1)	PE-13 (1) (2)
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 Applicable	PE-17	PE-17

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, physical and environmental protection policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policies and associated physical and environmental protection controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-28, *Physical and Environmental Protection*, describes the DOE criteria for physical and environmental protection controls.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Develop and keep current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the operating unit review and approve the access list and authorization credentials [*at least annually*].

DOE Manual 470.4-2, *Physical Protection*, and DOE Notice 206.3, *Personal Identity Verification*, also contain DOE requirements related to authorization credentials and their issuance.

PE-3 PHYSICAL ACCESS CONTROL

Control all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verify individual access authorizations before granting access to the facilities. The operating units also control access to areas officially designated as publicly accessible, as appropriate, in accordance with the operating unit's assessment of risk.

DOE Manual 470.4-2, *Physical Protection*, also contains DOE requirements pertaining to access controls.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control PE-4 is not required, at this time. Senior DOE Management PCSPs may specify or operating units may elect, at their discretion, to control physical access to information system transmission lines carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering.

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM

Control physical access to MODERATE- and HIGH-impact information system devices that display information to prevent unauthorized individuals from observing the display output.

PE-6 MONITORING PHYSICAL ACCESS

Monitor physical access to information systems to detect and respond to incidents.

- (1) Monitor real-time intrusion alarms and surveillance equipment for MODERATE- and HIGH-impact information systems.
- (2) Employ automated mechanisms to recognize potential intrusions and initiate appropriate response actions for HIGH-impact information systems.

PE-7 VISITOR CONTROL

Control physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.

- (1) Escort visitors and monitor visitor activity to MODERATE- and HIGH-impact information systems, when required.

DOE Manual 470.4-2, *Physical Protection*, also contains DOE requirements related to controlling visitor access to certain security areas.

PE-8 ACCESS LOGS

Maintain a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the access logs [*in a timely manner, as specified by each operating unit*], after closeout.

DOE Manual 470.4-2, *Physical Protection*, also contains DOE requirements for monitoring visitor access logs.

- (1) Employ automated mechanisms to facilitate the maintenance and review of access logs for MODERATE- and HIGH-impact information systems.

PE-9 POWER EQUIPMENT AND POWER CABLING

Protect power equipment and power cabling from damage and destruction for MODERATE- and HIGH-impact information systems.

Senior DOE Management should consider recommending that each operating unit employ redundant and parallel power cabling paths for HIGH-impact information systems.

PE-10 EMERGENCY SHUTOFF

Provide the capability of shutting off power to any for MODERATE- and HIGH-impact information system component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

PE-11 EMERGENCY POWER

Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of MODERATE- and HIGH-impact information system in the event of a primary power source loss.

- (1) Provide a long-term alternate power supply for HIGH-impact information systems that are capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Senior DOE Management should consider recommending that each operating unit provide a long-term alternate power supply for HIGH-impact

information systems that is self-contained and not reliant on external power generation.

PE-12 EMERGENCY LIGHTING

Employ and maintain automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.

PE-13 FIRE PROTECTION

Employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.

- (1) Configure fire suppression and detection devices/systems to activate automatically in the event of a fire for MODERATE- and HIGH-impact information systems.
- (2) Configure fire suppression and detection devices/systems to provide automatic notification of any activation to the organization and emergency responders for HIGH-impact information systems.

DOE Order 420.1B, *Facility Safety*, also contains DOE requirements for fire protection.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Regularly maintain within acceptable levels and monitor the temperature and humidity within facilities containing information systems.

PE-15 WATER DAMAGE PROTECTION

Protect the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.

- (1) Employ automated mechanisms to automatically close shutoff valves in the event of a significant water leak for HIGH-impact information systems.

PE-16 DELIVERY AND REMOVAL

Control information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintain appropriate records of those items.

PE-17 ALTERNATE WORK SITE

Require that individuals within the operating unit employ appropriate cyber security controls at alternate work sites for MODERATE- and HIGH-impact information systems.

19. PLANNING CONTROLS.

In their PCSPs, Senior DOE Management are to address the planning controls listed in **Table 13** for all general support systems and major applications under their responsibility.

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	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-25, *Security Planning Controls*, describes the DOE criteria for planning controls.

PL-2 SYSTEM SECURITY PLAN

Develop and implement a security plan for each 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.

PL-3 SYSTEM SECURITY PLAN UPDATE

Define and document procedures to require a review of each system security plan [*at least annually*] as part of system [self-assessments](#) and to revise the plan to address [significant changes](#) and problems identified during plan implementation or security control assessments

PL-4 RULES OF BEHAVIOR

Establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to 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, including consent to monitoring, before authorizing access to the information system.

PL-5 PRIVACY IMPACT ASSESSMENT

Conduct a privacy impact assessment on applicable information systems, as defined in the PCSP.

NOTE: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

20. PERSONNEL SECURITY.

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. In their PCSPs, Senior DOE Management are to address the personnel security controls listed in Table 14.

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	PS-2
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

Personnel Security				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
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

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, personnel security policies that address purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policies and associated personnel security controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-27, *Personnel Security*, describes the DOE criteria for personnel security.

PS-2 POSITION CATEGORIZATION

Assign a risk designation to all positions and establish screening criteria for individuals filling those positions. The Senior DOE Management operating unit Chief Information Officer (or equivalent), in coordination with the operating unit's Office of Human Resources, Office of Security, and Office of Acquisition Management reviews and revises position risk designations on a sampling basis [*at least every 3 years*].

PS-3 PERSONNEL SCREENING

Require all personnel be subject to an appropriate screening process prior to permitting permanent access to information and information system resources. *Screening must be performed for operating unit employees, contractors, and any "guests" prior to their being given access to operating unit systems and networks. A risk-based, cost-effective approach must be followed to determine the risk of harm to the system in comparison to the opportunity for personnel performing the following functions:*

- *Personnel 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).

- *User with root access to MODERATE- OR HIGH-impact information systems who may modify core data stores, 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.*
- *Users with access to an operating unit local area network, e-mail, basic office applications (such as Microsoft Office or Corel Office suites), and 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).*

DOE Notice 206.3, *Personal Identity Verification*, also contains requirements for personnel screening related to issuing DOE security badges.

PS-4 PERSONNEL TERMINATION

When employment is terminated, terminate user information system access, conduct exit interviews, and ensure the return all organizational information system-related property (e.g., keys, identification cards, building passes) in a timely manner. Appropriate personnel are to be granted access to all official records created by the terminated employee that are stored on organizational information systems before the systems are recycled or disposed.

DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*, and DOE Manual 470.4-2, *Physical Protection*, also contain requirements pertaining to terminating personnel.

PS-5 PERSONNEL TRANSFER

Review information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations). A change in user access and, therefore, suitability and risk may arise when an individual changes job duties within an operating unit or changes operating units.

DOE Manual 470.4-2, *Physical Protection*, also contains requirements pertaining to transferring personnel.

PS-6 ACCESS AGREEMENTS

Complete appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for

all individuals requiring access to organizational information and information systems before authorizing access.

PS-7 THIRD-PARTY PERSONNEL SECURITY

Comply with the personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) established by Senior DOE Management PCSP and monitor provider compliance to ensure adequate security.

PS-8 PERSONNEL SANCTIONS

Comply with the formal sanctions process for personnel failing to comply with established information security policies and procedures established by the Senior DOE Management PCSP.

DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*, also contains requirements associated disciplinary actions for information security related incidents.

21. RISK ASSESSMENT.

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.

In their PCSPs, Senior DOE Management are to address the controls listed in Table 15 for risk assessment of all General Support Systems and Major Applications under their responsibility.

Table 15. Controls for Risk Assessment

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

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-3, *Risk Management*, describes the criteria for implementing a risk management approach for all information systems within DOE.

RA-2 SECURITY CATEGORIZATION

Define and document procedures to require that the information system and the information processed, stored, or transmitted by the system is categorized in accordance with FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, and document the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization must review and approve the security categorizations.

NOTE: NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume I and Volume II, provides guidance on the assignment of security categories to information systems.

RA-3 RISK ASSESSMENT

Conduct 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 operating unit.

RA-4 RISK ASSESSMENT UPDATE

Update the information system risk assessments at least every 3 years or whenever there is a significant change to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

RA-5 VULNERABILITY SCANNING

Use appropriate vulnerability scanning tools and techniques to scan for vulnerabilities in Low-impact information systems [*at least quarterly*] or when significant new vulnerabilities affecting the system are identified and reported

- (1) For MODERATE- and HIGH-impact information systems, use appropriate vulnerability scanning tools and techniques to scan for vulnerabilities at least quarterly.
- (2) For HIGH-impact information systems, use information system vulnerability scanning tools and techniques that include the capability to readily update the list of vulnerabilities scanned; and that the vulnerability scanning procedures include means to ensure the adequacy of scan coverage, for both the vulnerabilities checked and the information system components scanned.

NOTE: DOE CIO Guidance CS-4, *Vulnerability Scanning*, describes the DOE criteria for vulnerability scanning for all information systems within DOE.

22. SYSTEM AND SERVICES ACQUISITION.

In their PCSPs, Senior DOE Management are to address the system and service acquisition controls listed in Table 16 for all general support systems and major applications under their responsibility.

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	SA-4	SA-4
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)

System and Services Acquisition				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
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 Design Principles	Not Applicable	SA-8	SA-8
SA-9	Outsourced Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Applicable	Not Applicable	SA-10
SA-11	Developer Security Testing	Not Applicable	SA-11	SA-11

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-26, *Systems and Services Acquisition*, describes the DOE criteria for the acquisition of systems and services.

SA-2 ALLOCATION OF RESOURCES

Determine, document, and allocate as part of its capital planning and investment control process the resources required to adequately protect the information system.

SA-3 LIFE CYCLE SUPPORT

Manage information systems using a system development life cycle methodology that includes information security considerations.

SA-4 ACQUISITIONS

Include security requirements and/or security specifications, either explicitly or by reference, in information system [*and information technology service*] acquisition contracts based on an assessment of risk.

SA-5 INFORMATION SYSTEM DOCUMENTATION

Ensure that adequate documentation for their information systems and constituent components is available, protected when required, and distributed to authorized personnel.

- (1) Document the functional properties of the security controls employed within MODERATE and HIGH-impact systems with sufficient detail to permit analysis and testing of the controls is available.
- (2) Document the design and implementation details of the security controls employed within HIGH-impact information systems with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components) is available.

SA-6 SOFTWARE USAGE RESTRICTIONS

Comply with software usage restrictions established in the Senior DOE Management PCSP.

SA-7 USER INSTALLED SOFTWARE

Enforce explicit rules governing the downloading and installation of external software by users. See control SA-10 for management of internally developed software.

SA-8 SECURITY DESIGN PRINCIPLES

Design and implement the information system using security engineering principles. Senior DOE Management should consider recommending that each operating unit design and implement the information system using security engineering principles as recommended in NIST SP 800-27A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security) Revision A*.

SA-9 OUTSOURCED INFORMATION SYSTEM SERVICES

Ensure that third-party providers of information system services employ adequate security controls in accordance with applicable Federal laws, Directives, policies, regulations, standards, guidance, and established service level agreements. Senior DOE Management PCSPs are to require each operating unit to monitor security control compliance for outsourced services.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

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.

SA-11 DEVELOPER SECURITY TESTING

Create a security test and evaluation plan, implement the plan, and document the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.

23. SYSTEM AND COMMUNICATIONS PROTECTION.

In their PCSPs, Senior DOE Management are to address the system and communications protection controls listed in **Table 17** for all general support systems and major applications under their responsibility.

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 Applicable	SC-2	SC-2
SC-3	Security Function Isolation	Not Applicable	Not Applicable	SC-3
SC-4	Information Remnants	Not Applicable	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Applicable	SC-6	SC-6
SC-7	Boundary Protection	SC-7	SC-7 (1)	SC-7 (1)
SC-8	Transmission Integrity	Not Applicable	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Applicable	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Applicable	SC-10	SC-10
SC-11	Trusted Path	Not Applicable	Not Applicable	Not Applicable
SC-12	Cryptographic Key Establishment and Management	Not Applicable	SC-12	SC-12
SC-13	Use of Validated Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Applicable	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Applicable	Not Applicable	Not Applicable
SC-17	Public Key Infrastructure Certificates	Not Applicable	SC-17	SC-17
SC-18	Mobile Code	Not Applicable	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Applicable	SC-19	SC-19

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, system and communications protection policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-35, *System and Communication Protection*, describes the DOE criteria for system and communication protection controls.

SC-2 APPLICATION PARTITIONING

For MODERATE- and HIGH-impact information systems, separate user functionality (including user interface services) from information system management functionality.

SC-3 SECURITY FUNCTION ISOLATION

For HIGH-impact systems, isolate 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 must maintain a separate execution domain (e.g., address space) for each executing process.

SC-4 INFORMATION REMNANTS

For MODERATE- and HIGH-impact information systems, prevent unauthorized and unintended information transfer via shared system resources.

SC-5 DENIAL OF SERVICE PROTECTION

Protect against or limit the effects of [*the types of denial of service attacks listed in the information system SSP*] for all information systems. Senior DOE Management should consider recommending that information systems:

- Restrict the ability of users to launch denial of service attacks against other information systems or networks.
- Manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

SC-6 RESOURCE PRIORITY

For MODERATE- and HIGH-impact information systems, limit the use of resources by priority.

SC-7 BOUNDARY PROTECTION

Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.

- (1) Physically allocate publicly accessible MODERATE- and HIGH-impact information systems components (e.g., public web servers) to separate sub-networks with separate, physical network interfaces. The Senior DOE Management operating unit must prevent public access into the organization's internal networks except as appropriately mediated.

SC-8 TRANSMISSION INTEGRITY

For MODERATE- and HIGH-impact information systems, protect the integrity of transmitted information.

- (1) Employ cryptographic mechanisms for HIGH-impact information systems to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).

SC-9 TRANSMISSION CONFIDENTIALITY

For MODERATE- and HIGH-impact information systems, protect the confidentiality of transmitted information.

- (1) Employ cryptographic mechanisms for HIGH-impact information systems to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).

SC-10 NETWORK DISCONNECT

For MODERATE- and HIGH-impact information systems, terminate a network connection at the end of a session or [*after a time specified in the information system SSP*].

SC-11 TRUSTED PATH

Control AC-11 is required, at this time. Senior DOE Management PCSPs may specify or operating units elect, may, at their discretion, to ensure that information systems establish a trusted communications path between the user and the security functionality of the system.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management for MODERATE- and HIGH-impact information systems.

SC-13 USE OF VALIDATED CRYPTOGRAPHY

When cryptography is employed within the information system, perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

SC-14 PUBLIC ACCESS PROTECTIONS

For publicly available systems, protect the integrity of the information and applications.

SC-15 COLLABORATIVE COMPUTING

For MODERATE- and HIGH-impact information systems, prohibit remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provide an explicit indication of use to the local users (e.g., use of camera or microphone).

SC-16 TRANSMISSION OF SECURITY PARAMETERS

Control AC-16 is not required, at this time. Senior DOE Management PCSPs may specify or operating units may elect, at their discretion, to ensure that information systems reliably associate security parameters (e.g., security labels and markings) with information exchanged between information systems.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in MODERATE- and HIGH-impact systems.

SC-18 MOBILE CODE

For MODERATE- and HIGH-impact systems: (i) establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) document, monitor, and control the use of mobile code within the information system.

SC-19 VOICE OVER INTERNET PROTOCOL

For MODERATE- and HIGH-impact systems: (i) establish 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; and (ii) document, monitor, and control the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.

DOE CIO Guidance CS-16, *Voice Over IP Systems*, describes the DOE criteria for using voice over Internet protocol technologies within DOE.

24. SYSTEM AND INFORMATION INTEGRITY.

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. In their PCSPs, Senior DOE Management are to address the system and information integrity controls listed in **Table 18** for all general support systems and major applications under their responsibility.

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	SI-2	SI-2 (1)
SI-3	Malicious Code Protection	SI-3	SI-3 (1)	SI-3 (1) (2)
SI-4	Intrusion Detection Tools and Techniques	SI-4	SI-4	SI-4 (1)
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)
SI-7	Software and Information Integrity	Not Applicable	Not Applicable	SI-7
SI-8	Spam and Spyware Protection	SI-8	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Applicable	SI-9	SI-9
SI-10	Information Input Accuracy, Completeness, and Validity	Not Applicable	SI-10	SI-10
SI-11	Error Handling	Not Applicable	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Applicable	SI-12	SI-12

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Each Senior DOE Management organization is to develop, document in its PCSP, disseminate, and periodically review/update: (i) formal, documented, system and information integrity policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policies and associated system and information integrity controls for all information systems in all Senior DOE Management operating units.

NOTE: DOE CIO Guidance CS-30, *System and Information Integrity*, describes the DOE criteria for system and information integrity controls.

SI-2 FLAW REMEDIATION

Identify and correct information system flaws and share information on flaws identified with the DOE Cyber Incident Capability.

(1) For HIGH-impact information systems:

- Centrally manage the flaw remediation process and install updates automatically without individual user intervention.
- Employ automated mechanisms to periodically and, upon command, determine the state of information system components with regard to flaw remediation.

SI-3 MALICIOUS CODE PROTECTION

Implement malicious code protection that includes a capability for automatic updates.

- (1) Centrally manage virus protection mechanisms for MODERATE- and HIGH-impact information systems.
- (2) Employ malicious code protection that automatically updates virus protection mechanisms for HIGH-impact information systems.

SI-4 INTRUSION DETECTION TOOLS AND TECHNIQUES

Employ tools and techniques to monitor events, detect attacks, and provide identification of unauthorized use of the system.

Consistent with the recommendations in this Guidance, all Senior DOE Management PCSPs are to require Internet access points to have network-based intrusion detection systems and require all Internet-accessible operating unit web servers to have host-based intrusion detection systems in place and functioning.

- (1) For HIGH-impact information systems, the Senior DOE Management PCSP should recommend:
- Networking individual intrusion detection tools into a system-wide intrusion detection system using common protocols.
 - Employing automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
 - Employing 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.
 - Monitoring outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).

NOTE: DOE CIO Guidance CS-9, *Incident Prevention, Warning, and Response Guidance*, describes criteria for cyber security incidents for all information systems within DOE.

SI-5 SECURITY ALERTS AND ADVISORIES

Receive cyber security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

- (1) Employ automated mechanisms for HIGH-impact information systems to make security alert and advisory information available throughout the organization as needed.

NOTE: DOE CIO Guidance CS-9, *Incident Prevention, Warning, and Response (IPWAR) Guidance*, describes criteria for cyber security incidents for all information systems within DOE.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Document security functionality controls in their procedures and information systems verify the correct operation of security functions [*either upon system startup and restart, upon command by user with appropriate privilege,*] or [*at least quarterly*]; and [*either notifies system administrator, shuts the system down, or restarts the system*] when anomalies are discovered.

- (1) The Senior DOE Management PCSP should recommend, for HIGH-impact information systems:
- Employment of automated mechanisms to provide notification of failed security tests.

- Employment of automated mechanisms to support management of distributed security testing.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

For HIGH-impact information systems detect and protect against unauthorized changes to software and information.

SI-8 SPAM AND SPYWARE PROTECTION

Implement SPAM and spyware protection if the system is vulnerable to these threats. If the system is not affected by these threats, define procedures to ensure that the resistant characteristics are documented in the system security plan.

- (1) Centrally manage spam and spyware protection mechanisms for HIGH-impact information systems.

The Senior DOE Management PCSP should recommend that each operating unit ensure HIGH-impact information systems automatically update SPAM and spyware protection mechanisms.

SI-9 INFORMATION INPUT RESTRICTIONS

Restrict the information input to authorized personnel only for MODERATE- and HIGH-impact information systems.

SI-10 INFORMATION INPUT ACCURACY, COMPLETENESS, AND VALIDITY

MODERATE- and HIGH-impact information systems check information inputs for accuracy, completeness, and validity.

SI-11 ERROR HANDLING

MODERATE- and HIGH-impact information systems identify and handle error conditions in an expeditious manner.

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Handle and retain output from MODERATE- and HIGH-impact information systems in accordance with Departmental, Senior DOE Management, and operating unit policy and operational requirements.

25. REFERENCES.

References are defined in Attachment 2.

26. DEFINITIONS.

Acronyms and terms are defined in Attachments 3 and 4.

27. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO
GUIDANCE CS-1 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2REFERENCES

Note: This attachment contains references for all DOE CIO Guidance. Individual guidance documents will refer to this attachment for most references. Each guidance document will contain only those references unique to that document.

U.S. Public Laws

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

Information Technology Management Reform Act of 1996 (Public Law 104-106), August 1996.

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

Office of Management and Budget (OMB)

Circular A-130, *Management of Federal Information Resources* - This Circular establishes policy for the management of Federal information resources in accordance with the Computer Security Act of 1987.

Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, November 2000. This Appendix assigns Federal Agency responsibilities for the security of automated information and incorporates requirements of the Computer Security Act of 1987 and responsibilities assigned in applicable national security Directives

Department of Energy Orders, Manuals, Notices, and Guidelines

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

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

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

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

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

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

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

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

DOE N 221.8, Reporting Fraud, Waste, and Abuse, dated 7-29-02.

DOE N 471.3, Reporting Incidents of Security Concern, dated 4-13-01.

DOE 5670.3, Counterintelligence Program, dated 9-04-92.

Other

Executive Order (EO) 13231, *Critical Infrastructure Protection in the Information Age* (October 16, 2001) - The purpose of this order is to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and Government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible.

EO 13011, *Federal Information Technology*, dated 7-17-96.

EO 12344, *Naval Nuclear Propulsion Program*, dated 2-1-82.

EO 12958, *Classified National Security Information*, dated 4-17-95.

Homeland Security Presidential Directive (HSPD)-7, *Critical Infrastructure Identification, Prioritization, and Protection* (December 17, 2003) superseded The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (May 22, 1998) to ensure the viability of national infrastructures that are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004)

National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems*. This Directive establishes initial objectives of policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation.

Issuances of the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC), [Policies (P), Directives (D), and Instructions (I)]

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

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

NIST FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

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

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

NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

NIST SP 800-27A, *Engineering Principles for Information Technology Security*, Revision A, June 2004

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

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

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

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

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

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

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

NIST SP 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, April 2006.

ATTACHMENT 3ACRONYMS

Note: This attachment contains acronyms for all DOE CIO Guidance documents. Individual guidance documents will refer to this attachment for most acronyms. Each guidance document will contain only those acronyms unique to the specific guidance document.

C&A	Certification and accreditation
CIO	Chief Information Officer
CNSS	Committee for National Security Systems
DAA	Designated Approving Authority
E.O.	Executive Order
FIPS	Federal Information Processing Standards
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
ISSO	Information systems security officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PCSP	Program Cyber Security Plan
P.L.	Public Law
SSP	System Security Plan
ST&E	Security Testing And Evaluation
U.S.C.	United States Code

ATTACHMENT 4GLOSSARY

Note: This attachment contains terms for all DOE CIO Guidance documents. Individual guidance documents will refer to this attachment for most terms. Each guidance document will contain only those terms unique to the specific guidance document.

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

Accreditation Boundary: All components of an information system to be accredited by an authorizing official, excluding separately accredited systems, to which the information system is connected. *Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.*

Accreditation Official: See Authorizing Official.

Adequate Security: Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [OMB Circular A-130, Appendix III].

Agency: Any Executive Department, military department, Government corporation, Government controlled corporation, or other establishment in the Executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include: (i) the Government Accountability Office; (ii) the Federal Election Commission; (iii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (iv) government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. [44 U.S.C., SEC. 3502]

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, ensure compliance with established policies and operational procedures, and recommend necessary changes in controls, policies, or procedures.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. 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).

Authorizing Official: Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals. *Synonymous with Accreditation Authority. Also referred to as the Designated Approving Authority*

(DAA), the authorizing official (or approving/accrediting authority) must be a senior DOE program official or other DOE executive.

Availability: Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

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

Certification Agent (Certifier): An individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome in meeting system security requirements.

Chief Information Officer: Agency official responsible for: (i) providing advice and other assistance to the head of the Executive Agency and other senior management personnel of the Agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the Agency; (ii) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the Agency; and (iii) promoting the effective and efficient design and operation of all major information resources management processes for the Agency, including improvements to work processes of the Agency. [44 U.S.C., Sec. 5125(b)]

Classified Information: Restricted Data or Formerly Restricted Data as defined under the Atomic Energy Act of 1954, as amended; or information that requires protection against unauthorized disclosure per Executive Order 12958 or prior Executive orders and is marked to indicate its classified status when in documentary form.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]

Countermeasures: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. [CNSS Instruction 4009] *Synonymous with security controls and safeguards.*

Critical Infrastructure Protection: Continuous efforts to secure information systems for critical infrastructure, emergency preparedness communications, and the physical assets that support such systems.

Designated Approving Authority (DAA): See authorizing official.

DOE Organizations: Primary programs and administrations that make up DOE. See Attachment 1 of this Order.

Environment: Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. [CNSS Instruction 4009]

Executive Agency: An Executive Department specified in 5 U.S.C., SEC. 101; a military department specified in 5 U.S.C., SEC. 102; an independent establishment as defined in 5 U.S.C., SEC. 104(1); and a wholly-owned Government corporation fully subject to the provisions of 31 U.S.C., CHAPTER 91. [41 U.S.C., SEC. 403]

Federal Agency: See Agency.

Federal Information System: An information system used or operated by an Executive Agency, by a contractor of an Executive Agency, or by another organization on behalf of an Executive Agency. [40 U.S.C., SEC. 11331]

General Support System: An interconnected information resource that share common functionality and operate under the same direct management control; includes hardware, software, information, data, applications, communications, and people. A system, for example, can be a local area network and smart terminals that support a branch office; a communications network; a data processing center, operating system, and utilities; a tactical radio network; or shared information processing services. (OMB Circular A-130, Appendix III)

Heads of Primary DOE Organizations: Primary managers of DOE programs; at Headquarters, the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and staff office directors); in the field, managers of the eight operations offices and the three field offices and administrators of the power marketing administrations.

High-Impact System: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information: An instance of an information type. [FIPS Publication 199]

Information Owner: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSS Instruction 4009]

Information Resources: Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., SEC. 3502]

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., SEC. 3542]

Integration Testing – The process of testing a system component or module after it has been combined or interconnected with a larger system infrastructure to ensure all components function as intended and are interoperable. For example, software integration testing verifies that units of software, when combined, work together as intended so that interfaces work correctly. Similarly, system interoperability testing verifies that a defined set of interrelated systems, which collectively support an organizational core business function, interoperate as intended with each other and with external interfaces in an operational environment (either actual or simulated).

Information System (IS): A discrete set of Order or automated resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures. Information systems include personnel, hardware, software, and procedures that support the operation of the system.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., SEC. 3502]

Information System Owner: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [CNSS Instruction 4009 Adapted]

Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Executive Agency. For purposes of the preceding sentence, equipment is used by an Executive Agency if the equipment is used by the Executive Agency directly or is used by a contractor under a contract with the Executive Agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources and does not include equipment acquired incidental to a Federal contract or national security information systems as defined in the Clinger Cohen Act of 1996 (P. L. 104-106) and OMB Circular A-130, Appendix III. [40 U.S.C., SEC. 1401]

Information Type: A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or, in some instances, by a specific law, Executive Order, Directive, policy, or regulation. [FIPS Publication 199]

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

IT Resources – IT resources consist of computer hardware, software, firmware, electronic data, networks, and support for these assets.

Local Area Network (LAN) – Computer network that spans a relatively small area, such as a single building or group of buildings.

Low-Impact System: An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Management Controls: The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Major Application: One that requires special security because of its potential for risk and magnitude of harm resulting from the loss, misuse, modification, or unauthorized access to information in the application. (NOTE: All Federal applications require some level of protection.) Some applications require special management oversight and should be treated as major applications. Adequate security for other applications is provided by the security of the systems in which they operate. (OMB Circular A-130, Appendix III)

Management Controls: The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of cyber security. They consist of: risk assessment; planning; system and services acquisition; and certification, accreditation, and security assessment.

Material Weakness: As defined in OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, a cyber security material weakness is a significant deficiency in IT security policy, procedures, or practices, such as absence of system security plans and failure to properly certify and accredit systems before operation.

Media: Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Moderate-Impact System: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.

National Security Information: Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System: Any information system (including any telecommunications system) used or operated by an Agency or by a contractor of an Agency, or other organization on behalf of an Agency— (i) the function, operation, or use of which involves

intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [44 U.S.C., SEC. 3542]

Occurrence: An (i.e., recurring) event or condition that will or may adversely affect DOE contractor personnel, the public, property, the environment, or the DOE mission. Events or conditions meeting criteria identified in DOE M 231.1-2 or determined through performance analysis to have potential for recurrence.

Operational Control: The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). They consist of: personnel security; physical and environmental protection; contingency planning; configuration management; maintenance; system and information integrity; media protection; incident response; and awareness and training.

Operating Unit: 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.

Organization: A Federal Agency or, as appropriate, any of its operational elements.

Potential Impact: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. [FIPS Publication 199]

Records: All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that Agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them. [44 U.S.C. SEC. 3301]

Residual Risk: The portion remaining after security measures have been applied.

Risk: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational 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 Assessment: The process of identifying risks to organization / Agency operations

(including mission, functions, image, or reputation), Agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, *synonymous with risk analysis*, and incorporates threat and vulnerability analyses.

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [CNSS Instruction 4009 Adapted] *Synonymous with security controls and countermeasures.*

Sanitization: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. [CNSS Instruction 4009 Adapted]

Security Category: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. [FIPS Publication 199]

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS Publication 199]

Security Control Baseline: The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Test and Evaluation (ST&E): ST&E is the process used to examine the effectiveness of information system controls with the objective of determining the true risk, or exposure, of the system to certain threats. Through the conduct of control tests, vulnerabilities are identified that result from improper use of controls, missing controls, inherent system vulnerabilities, or mismanagement. Through the application of ST&E methods, the certification agent analyzes the current state of the system by reviewing the system objects, and searching for anomalies that might indicate vulnerabilities that could permit an attack. ST&E results in development of a plan of actions and milestones to track corrective actions necessary to mitigate vulnerabilities and reduce risk.

Security Objective: Confidentiality, integrity, or availability. [FIPS Publication 199]

Security Plan: See System Security Plan.

Security Requirements: Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Senior Agency Information Security Officer: Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the Agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544]

Senior DOE Management: DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, Heads of DOE Elements with subordinate units outside of DOE Headquarters, and DOE Chief Information Officer

Senior Program Officials: Senior program officials are upper-level managers in charge of line offices who directly report to the Operating Unit Head. For example, if the Operating Unit Head is an Under Secretary, then the senior program officials are the assistant secretaries or office directors, as applicable; if the Operating Unit Head is a Director, then the senior program officials are the associate directors.

Security: Measures and controls that ensure the confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

Social Engineering: Techniques that rely on weaknesses in human nature rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security.

Significant Change: A significant change is one that alters the baseline system configuration through the addition, deletion, or change of a configuration item within the system. Examples of significant changes to an information system that should be reviewed for possible re-accreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a re-accreditation action.

System: See information System.

System Certifier: See certification agent.

System Security Plan: Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [NIST Special Publication 800-18, Revision 1]

System Owner: Mid-level manager responsible for day-to-day system operations and responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Technical Controls: The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. They consist of: identification and authentication; access control; audit and accountability; and system and communications protection.

Technical Controls: The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. For example,

- External security threats from individuals who use technical knowledge or social engineering to gain unauthorized access (via remote access or by gaining local access) to perform malicious activity in cyber systems.
- Insider security threats (intentional or unintentional) have the potential to be more serious than external threats because the perpetrator has authorized access to the system.
- Foreign access threat (remote or internal) to the information environment requiring assessment to ensure foreign nationals' access to DOE cyber systems is approved by an official designated by the DOE site manager or line-level organization accountable for the approval decision.
- Portable electronic devices (laptop computers, palm devices, and cell phones) capable of receiving, storing, or transmitting data in an electronic format. Issues of concern include data aggregation, theft, and radio frequency/infrared interconnectivity.
- Mosaic threat that classified information or information requiring enhanced protection will be derived by combining open source information made separately available, perhaps by different organizations.

Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. [CNSS Instruction 4009 Adapted]

Threat Assessment: Formal evaluation and description of potential for threat to an information system.

Threat Source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. *Synonymous with threat agent.*

Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, or other resource. For example,

- An attacker runs an exploit tool to gain access to a server's password file.
- A perpetrator obtains unauthorized administrator-level access to a system and then threatens the victim that the details of the break-in will be released to the press if the organization does not pay a designated sum of money.

Unclassified Information: Information designation for a document or material that has been determined not to be classified or that has been declassified by proper authority.

Unclassified Controlled Information: A document or material that may be exempt from public release under the Freedom of Information Act or other statute (e.g., Official Use Only information, Unclassified Controlled Nuclear Information).

User: Individual or (system) process authorized to access an information system. [CNSS Instruction 4009]

Vulnerability: Weakness in an information system, security procedure, internal control, or process implementation that could be exploited or triggered by a threat source [CNSS Instruction 4009 Adapted], as follows.

- Major vulnerability, which if discovered and exploited, could reasonably be expected to result in a successful attack causing serious damage to the national security.
- Unspecified major vulnerability in a system or organization's defenses that could be exploited and is specified in no greater detail than the specific security system (or one of its major components) when it occurs.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [CNSS Instruction 4009 Adapted]

Vulnerability Assessment: Systematic examination of an information system or product to determine adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Wide Area Network (WAN): A wide area network is a system of LANs connected to other LANs over any distance via telephone lines and radio waves.

Wireless LAN (WLAN): A wireless LAN consists of a network that uses radio waves rather than wires to communicate between nodes.