Cyber Security Technical and Management Requirements

Management, Operational, and Technical Controls (TMR-1)
October 10, 2007

Department of Energy (DOE) Order 205.1A, *Department of Energy Cyber Security Management*, charges Senior DOE Management to implement cyber security within their respective organizations, based on their determination, assessment, and documentation of DOE and program-unique threats and risks. In carrying out this charge, Senior DOE Management is required by the Order to develop a Program Cyber Security Plan (PCSP) that defines cyber security requirements for all subordinate organizations and programs. The Order requires that the PCSP requirements comply with the Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, Office of Management and Budget (OMB) directives, Federal Information Processing Standards (FIPS), Departmental policies, and DOE Chief Information Officer (CIO) Cyber Security Technical and Management Requirements (TMRs).

The selection and specification of security controls for an information system is accomplished as part of a management, operational, and technical process that include management of organizational risks and the risks in each system. This process is intended to result in adequate security controls for each system to ensure an acceptable level of residual risk.

In accordance with DOE O 205.1A, this TMR documents minimum Departmental criteria for the implementation of certain of the management, operations, and technical controls requirements defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, for unclassified information systems. The enhancements to the controls are determined from an analysis of numerous sources, including Plan of Action and Milestones (POA&M) and incident trending data, OMB requirements, NIST and Committee on National Security Systems (CNSS) documents, etc. in consideration of Departmentwide risk and threat assessment. These Departmental criteria are to be used by Senior DOE Management in providing implementation direction for NIST SP 800-53, Revision 1, in each PCSP. Senior DOE Management may specify and implement additional requirements in each PCSP to address specific risks, vulnerabilities, or threats within its operating units.

This TMR utilizes the NIST SP 800-53, Revision 1, structure utilizing the control Classes, Families, and Identifiers as shown in Table 1. Requirements TMR-1-2 through TMR-1-18 below include tables of all NIST SP 800-53, Revision 1, controls by family. If a security control is to be applied to system, the family identifier and control number are listed. If a control is not used, the cell is marked “not selected.” Control enhancements, when used to supplement basic security controls, are indicated parenthetically. Shaded cells in the tables indicate where controls have been modified for

Departmental use. For DOE-modified controls, the entire text of the control is included in this document, and changes to the control are highlighted with underline and **bold font**; refer to NIST SP 800-53, Revision 1, for the text of the controls that have not been modified for Departmental use.

Table 1. Cyber Security Control Classes, Families and Identifiers

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

Cancellations

This TMR replaces DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance,* dated July 6, 2006.

Implementation

This document defines management and technical cyber security requirements to be incorporated into Senior DOE Management PCSPs within 90 days of the TMR issue date.

Requirements

TMR-1-1, Managing Organizational Risk

Each Senior DOE Management organization is to document its approach to managing organizational risk through the organization's PCSP. Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing policies and processes to develop an acceptable control baseline for each unclassified information system appropriate to the impact level of the system (see Section 3.2, NIST SP 800-53, Revision 1, Security Categorization, for the process of categorizing system). The PCSP is also to describe the risk management or mission impact rationale for all controls not fully addressed in the PCSP.

Since the potential impact values for confidentiality, integrity, and availability may not be identical for an information system, the high-water mark concept is to be used to determine the impact level of the information system and select an initial set of security controls. To account for DOE-specific changes to the control sets, the PCSP is to apply the baselines defined in Tables 2 through 18 in this document. The baselines in this document, combined with the additional controls in NIST SP 800-53, Revision 1, establish the minimum sets of controls for all information systems processing unclassified information in DOE. Senior DOE Management can add new controls or modify the requirements for any specified control to a higher, but not lower, impact level.

TMR-1-2, Access Controls.

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. They include controls that restrict users to authorized transactions and functions and controls that limit network access and public accesses to the system. The Senior DOE Management PCSP is to address the access control controls listed in Table 2 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

Table 2. Access Controls

Access Controls				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3)(4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4

Access Controls				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7 **(1)**	AC-7 **(1)**
AC-8	System Use Notification	AC-8 **(1)**	AC-8 **(1)**	AC-8 **(1)**
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13(1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1)(2)(3)(4)	AC-17 (1)(2)(3)(4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1)(2)
AC-19	Access Control for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

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

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

Control Enhancements:

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

AC-8 SYSTEM USE NOTIFICATION

Control: The information system displays 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.

Supplemental Guidance: Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Control Enhancements:

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

****WARNING**WARNING**WARNING**WARNING**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-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for any user [*Assignment:* ***number of sessions, as defined in the information system SSP***]. Supplemental Guidance: None.

Control Enhancements: None.

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a remote session after [*Assignment:* ***time period specified in the information system SSP***].

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

Control Enhancements:

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

TMR-1-3, Awareness and Training Controls

Cyber security awareness consists of reminders that focus the user's attention on the concept of cyber security in the user's daily routine. Awareness provides a general cognizance or mindfulness of one's actions, and the consequences of those actions. Cyber security training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge, producing relevant and necessary security skills and competencies in those who access or manage DOE, including NNSA, information and resources. The Senior DOE Management PCSP is to address the awareness and training controls listed in Table 3 (extracted from NIST SP 800-53, Revision 1).

Table 3. Awareness and Training Controls

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

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) **within 30 days of appointment and** before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, **at least annually***] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

AT-3 SECURITY TRAINING

Control: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency, **at least every 2 years***] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the

organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

TMR-1-4, Audit and Accountability Controls

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can support individual accountability, a means to reconstruct events, detect intrusions, and identify problems. System audit trails, or event logs, provide a record of events in support of activities to monitor and enforce the information system security policy. NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, Chapter 18, describes an event as any action that happens on a computer system, such as logging into a system, executing a program, or opening a file. The Senior DOE Management PCSP is to address the audit and accountability controls listed in Table 4 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

Table 4. Audit and Accountability Controls

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

AU-2 AUDITABLE EVENTS

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

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

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

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

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

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

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

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related security control: AU-4.

Control Enhancements:

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

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

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

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

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

Control Enhancements:

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

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

AU-7 AUDIT REDUCTION AND REPORT GENERATION

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

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

Control Enhancements:

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

AU-11 AUDIT RECORD RETENTION

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

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

Control Enhancements: None.

TMR-1-5, Certification, Accreditation, and Security Assessments Controls

Certification and Accreditation (C&A) is the process of formal assessment, testing (certification), and acceptance (accreditation) of system security controls that protect information systems and data stored in and processed by those systems. It is a process that encompasses the system's life cycle and ensures that the risk of operating a system is recognized, evaluated, and accepted. The C&A process implements the concept of "adequate security," or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information, which is defined in OMB Circular A-130. The Senior DOE Management PCSP is to address the C&A and security assessment controls listed in Table 5 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

Table 5. Certification, Accreditation, and Security Assessments Controls

Certification, Accreditation, and Security Assessments				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	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 (1)	CA-4 (1)
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

TMR-1-6, Configuration Management Controls

The Senior DOE Management PCSP is to address the configuration management controls listed in Table 6 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications,

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 Selected	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1)(2)

CM-7 LEAST FUNCTIONALITY

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

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Control Enhancements:

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

TMR-1-7, Contingency Planning Controls.

Contingency Planning details the necessary procedures required to protect the continuing performance of core business functions and services, including information and information system services, during an outage. The Senior DOE Management PCSP is to address the contingency planning controls listed in Table 7 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

Table 7. Contingency Planning Controls

Contingency Planning				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1)(2)

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

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization: (i) tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.
Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Control Enhancements:

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

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

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

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

CP-7 ALTERNATE PROCESSING SITE

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

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

Control Enhancements:

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

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

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

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

CP-8 TELECOMMUNICATIONS SERVICES

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

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

Control Enhancements:

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

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

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

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

CP-9 INFORMATION SYSTEM BACKUP

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

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the

backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control. Related security controls: MP-4, MP-5.

Control Enhancements:

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

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

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

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

Enhancement Supplemental Guidance: The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control. Related security controls: MP-4, MP-5.

TMR-1-8, Identification and Authentication Controls

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an information system. Access control usually requires that the system be able to identify and differentiate among users. All DOE information systems must have 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. The Senior DOE Management PCSP is to address the identification and authentication controls listed in Table 8 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

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 (1)	IA-2 (2)(3)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication 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 identification and authentication policy and associated identification and authentication controls.

- **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 TMR-11, Password Management.**

Supplemental Guidance: The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-

78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

TMR-1-9, Incident Response Controls

An incident response capability is a mechanism through which an operating unit's system owners and Information System Security Officers are kept informed of system vulnerability advisories from the US-Computer Emergency Readiness Team (US-CERT), software vendors, and other sources. The capability also coordinates with responsible incident response capabilities regarding the handling and reporting of incidents involving systems under the operating unit's responsibility. An incident response capability may consist of one or more persons (such as the Information System Security Officer or CIO), who ensure that vulnerability advisories are communicated to system owners. The Senior DOE Management PCSP is to address the incident response controls listed in Table 9 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

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-2 INCIDENT RESPONSE TRAINING

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

Supplemental Guidance: None.

Control Enhancements:

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

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

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

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

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

Control Enhancements:

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

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

IR-5 INCIDENT MONITORING

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

Supplemental Guidance: None.

Control Enhancements:

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

TMR-1-10, Maintenance Controls

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. The process of configuration management provides for a controlled environment in which changes to hardware and software are properly authorized, tested, and approved before implementation. The Senior DOE Management PCSP is to address the maintenance controls listed in Table 10 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

Table 10. Maintenance Controls

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

MA-6 TIMELY MAINTENANCE

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

Supplemental Guidance: None.

Control Enhancements: None.

TMR-1-11, Media Protection Controls

DOE, including NNSA, requires that operating unit cyber security programs include procedures for storing, handling, and destroying national and non-national security information media. The Senior DOE Management PCSP is to address the media

protection controls listed in Table 11 (extracted from NIST SP 800-53, Revision 1) 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(1)	MP-2 (1)
MP-3	Media Labeling	Not Selected	**MP-3**	**MP-3**
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (1)(2)	MP-5 (1)(2)(3)
MP-6	Media Sanitization and Disposal	MP-6 **(1)(2)**	MP-6 **(1)(2)**	MP-6 (1)(2)

MP-3 MEDIA LABELING

Control: The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts [*Assignment: organization-defined list of media types, **documented the specific types of media or hardware components in the information system SSP***] exempt from labeling so long as they remain within [*Assignment: organization-defined protected environment*].

Supplemental Guidance: An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Control Enhancements: None.

MP-6 MEDIA SANITIZATION AND DISPOSAL

Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.

Supplemental Guidance: Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Control Enhancements:

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

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

TMR-1-12, Physical and Environmental Protection.
The Senior DOE Management PCSP is to address the physical and environmental controls listed in Table 12 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

Table 12. Physical and Environmental Protection Controls

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

Physical and Environmental Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
PE-8	Access Logs	PE-8	PE-8 **(1)**	PE-8 (1)(2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10 **(1)**	PE-10 (1)
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1)(2)(3)	PE-13 (1)(2)(3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18(1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

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

Supplemental Guidance: Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides. **DOE 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.**

Control Enhancements: None.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

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

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Control Enhancements: None.

PE-8 ACCESS RECORDS

Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (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 visitor access records [*Assignment: organization-defined frequency,* ***in a timely manner after closeout, as specified by the operating unit***].
Supplemental Guidance: None.

Control Enhancements:

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

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

PE-10 EMERGENCY SHUTOFF

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

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

Control Enhancements:

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

TMR-1-13, Planning Controls.
The Senior DOE Management PCSP is to address the planning controls listed in Table 13 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

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-6	Security Related Activity Planning	Not Selected	PL-6	PL-6

PL-5 PRIVACY IMPACT ASSESSMENT

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

Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002. **Departmental procedures for implementing OMB-M-03-22 are defined in *Department of Energy Procedures for Conducting Privacy Impact Assessments*, January 2007.**

Control Enhancements: None.

TMR-1-14, Personnel Security Controls.
Effective administration of users' computer access is essential to maintaining system security. Administration of system users focuses on identification, authentication, and access authorizations. DOE, including NNSA, requires that each operating unit implement and maintain a process of auditing and otherwise periodically verifying the

legitimacy of current accounts and access authorizations. In addition, they are to address the timely modification or removal of access and associated issues for employees who are reassigned, promoted, or terminated. Many important issues in computer security involve Federal and contractor system users, designers/programmers, implementers/maintainers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their job. No computer system can be secured without properly addressing these security issues. The Senior DOE Management PCSP is to address the personnel security controls listed in Table 14 (extracted from NIST SP 800-53, Revision 1).

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
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8

PS-2 POSITION CATEGORIZATION

Control: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [*Assignment: organization-defined frequency*, ***at least every 3 years***].

Supplemental Guidance: Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Control Enhancements: None.

PS-3 PERSONNEL SCREENING

Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access. **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).**
- **Users 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).**

Supplemental Guidance: Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position. **DOE Notice 206.4, *Personal Identity Verification*, also contains requirements for personnel screening related to issuing DOE security badges.**
Control Enhancements: None.

TMR-1-15, Risk Assessment Controls

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

A system owner, in consultation with the Information System Security Officer and other interested parties, such as the Designated Approving Authority, uses the results of this

evaluation to determine countermeasures to prevent or mitigate risk to an acceptable level. The Information System Security Officer can assist by providing the system owner with a risk assessment methodology and by providing assistance in interpreting the risk assessment results and suggesting possible cost-effective security countermeasure alternatives. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance, best practices, and sample templates for the risk assessment process. The Senior DOE Management PCSP is to address the controls listed in Table 15 (extracted from NIST SP 800-53, Revision 1) for risk assessment of all general support systems and major applications.

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-5 VULNERABILITY SCANNING

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

Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.

Control Enhancements:

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

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

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

TMR-1-16, System and Services Acquisition Controls.
The Senior DOE Management PCSP is to address the system and service acquisition controls listed in Table 16 for all general support systems and major applications.

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 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1)(2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11

SA-4 ACQUISITIONS

Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system **and**

information technology services acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance:

Solicitation Documents. The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

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

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

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

Control Enhancements:

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

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

TMR-1-17, System and Communications Protection Controls.
The Senior DOE Management PCSP is to address the system and communications protection controls listed in Table 17 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

Table 17. System and Communications Protection Controls

System and Communications Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	**SC-3**	SC-3
SC-4	Information Remnants	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1)(2)(3)(4)(5)	SC-7 (1)(2)(3)(4)(5) (6)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17

System and Communications Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name/Address Resolution Service (Authentication Source)	Not Selected	SC-20	SC-20
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Control Enhancements:

(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.

(2) The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.

(3) The information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

(4) The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.

(5) The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list,* ***as described in the information system SSP***].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

SC-7 BOUNDARY PROTECTION

Control: The information system monitors and controls communications at the **accreditation** boundary of the information system and at key internal boundaries within the system.

Supplemental Guidance: Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to

restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-77 provides guidance on virtual private networks. Related security controls: MP-4, RA-2.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces. Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

(2) The organization prevents public access into the organization's internal networks except as appropriately mediated.

(3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

(4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

(5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

(6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

SC-10 NETWORK DISCONNECT

Control: The information system terminates a network connection at the end of a session or after inactivity [*Assignment: organization-defined time period,* ***a time period specified in the information system SSP***].

Supplemental Guidance: The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Control Enhancements: None.

TMR-1-18, System and Information Integrity Controls

Integrity controls protect data in an information system from accidental or malicious alteration or destruction and provide assurance to the user that the information meets criteria about its quality and reliability. The Senior DOE Management PCSP is to address the system and information integrity controls listed in Table 18 (extracted from NIST SP 800-53, Revision 1) for all general support systems and major applications.

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 (2)	SI-2 (1)(2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1)(2)	SI-3 (1)(2)
SI-4	Information System Monitoring Tools and Techniques	**SI-4**	SI-4 (4)	SI-4 (2)(4)(5)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	**SI-6**	**SI-6**	SI-6 **(1)(2)**
SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7 (1)(2)
SI-8	Spam Protection	**SI-8**	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Input Accuracy, Completeness, and Validity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Supplemental Guidance: Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related security control: AC-8.

Control Enhancements:

(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

(2) The organization employs automated tools to support near-real-time analysis of events.

(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.

(5) The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system verifies the correct operation of security functions [*Selection (one or more): either upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: organization-defined time-period, **at least quarterly***]] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Control Enhancements:

(1) The organization employs automated mechanisms to provide notification of failed automated security tests.

(2) The organization employs automated mechanisms to support management of distributed security testing.

SI-8 SPAM PROTECTION

Control: The information system implements spam protection.

Supplemental Guidance: The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor

for workstations). NIST Special Publication 800-45 provides guidance on electronic mail security.

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The information system automatically updates spam protection mechanisms.