Annex 2 to NIST Special Publication 800-53

Recommended Security Controls for Federal Information Systems

Minimum Security Controls

Moderate Baseline

Includes updates through 04-22-2005

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AC-1	**ACCESS CONTROL POLICY AND PROCEDURES**	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	The access control policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control 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.
AC-2	**ACCOUNT MANAGEMENT**	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency*]. The organization employs automated mechanisms to support the management of information system accounts. The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*]. The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].	Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AC-3	**ACCESS ENFORCEMENT**	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).	Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 compliant.
AC-4	**INFORMATION FLOW ENFORCEMENT**	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Information flow control policies and enforcement mechanisms are employed by organizations to control the flow of information between designated sources and destinations (e.g., individuals, devices) within information systems and between interconnected systems based on the characteristics of the information. Simple examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Flow control enforcement can also be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions (e.g., to control the release of certain types of information).

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AC-5	SEPARATION OF DUTIES	The information system enforces separation of duties through assigned access authorizations.	The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.
AC-6	LEAST PRIVILEGE	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.
AC-7	UNSUCCESSFUL LOGIN ATTEMPTS	The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to* [*Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.	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.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AC-8	SYSTEM USE NOTIFICATION	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.	Privacy and security policies are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. For publicly accessible systems: (i) the system use information is available as opposed to displaying the information before granting access; (ii) there are no references to monitoring, recording, or auditing since privacy accommodations for such systems 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.
AC-11	SESSION LOCK	The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	Users can directly initiate session lock mechanisms. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system.
AC-12	SESSION TERMINATION	The information system automatically terminates a session after [*Assignment: organization-defined time period*] of inactivity.	None.
AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.	The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently, the activities of users with significant information system roles and responsibilities.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization identifies specific user actions that can be performed on the information system without identification or authentication. The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.	The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems.
AC-17	REMOTE ACCESS	The organization documents, monitors, and controls 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. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. The organization uses encryption to protect the confidentiality of remote access sessions. The organization controls all remote accesses through a managed access control point.	Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). The organization permits remote access for privileged functions only for compelling operational needs. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
AC-18	WIRELESS ACCESS RESTRICTIONS	The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies. The organization uses authentication and encryption to protect wireless access to the information system.	NIST Special Publication 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AC-19	ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES	The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.	Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are not allowed access to organizational networks without first meeting organizational security policies and procedures. Security policies and procedures might include such activities as scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).
AC-20	PERSONALLY OWNED INFORMATION SYSTEMS	The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.	The organization establishes strict terms and conditions for the use of personally owned information systems. The terms and conditions should address, at a minimum: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, spyware definitions).

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AT-1	**SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, 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.	The security awareness and training policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.
AT-2	**SECURITY AWARENESS**	The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and [*Assignment: organization-defined frequency, at least annually*] thereafter.	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 5 C.F.R. Part 930.301 and with the guidance in NIST Special Publication 800-50.
AT-3	**SECURITY TRAINING**	The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and [*Assignment: organization-defined frequency*] thereafter.	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 ensures system managers, system administrators, and other personnel having access to system-level software have adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in 5 C.F.R. Part 930.301 and with the guidance in NIST Special Publication 800-50.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AT-4	SECURITY TRAINING RECORDS	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.	None.
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability 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.
AU-2	AUDITABLE EVENTS	The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].	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. 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.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AU-3	CONTENT OF AUDIT RECORDS	The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events. The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.
AU-4	AUDIT STORAGE CAPACITY	The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.	None.
AU-5	AUDIT PROCESSING	In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)*].	None.
AU-6	AUDIT MONITORING, ANALYSIS, AND REPORTING	The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.	None.
AU-7	AUDIT REDUCTION AND REPORT GENERATION	The information system provides an audit reduction and report generation capability.	Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.
AU-8	TIME STAMPS	The information system provides time stamps for use in audit record generation.	Time stamps of audit records are generated using internal system clocks that are synchronized system wide.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
AU-9	PROTECTION OF AUDIT INFORMATION	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	None.
AU-11	AUDIT RETENTION	The organization retains audit logs for [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	NIST Special Publication 800-61 provides guidance on computer security incident handling and audit log retention.
CA-1	CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.	The security assessment and certification and accreditation policies and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on processing security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures.
CA-2	SECURITY ASSESSMENTS	The organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be tested with a frequency depending on risk, but no less than annually. NIST Special Publications 800-53A and 800-26 provide guidance on security control assessments.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
CA-3	INFORMATION SYSTEM CONNECTIONS	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.	Since FIPS 199 security categorizations apply to individual information systems, the organization should carefully consider the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations should also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on interconnecting information systems.
CA-4	SECURITY CERTIFICATION	The organization conducts 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.	A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is integrated into and spans the System Development Life Cycle (SDLC). NIST Special Publication 800-53A provides guidance on the assessment of security controls. NIST Special Publication 800-37 provides guidance on security certification and accreditation.
CA-5	PLAN OF ACTION AND MILESTONES	The organization develops and updates [*Assignment: organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
CA-6	SECURITY ACCREDITATION	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency*]. A senior organizational official signs and approves the security accreditation.	OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems.
CA-7	CONTINUOUS MONITORING	The organization monitors the security controls in the information system on an ongoing basis.	Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization establishes the selection criteria for control monitoring and subsequently selects a subset of the security controls employed within the information system for purposes of continuous monitoring. NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls.
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The configuration management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management 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.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
CM-2	BASELINE CONFIGURATION	The organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system's constituent components. The organization updates the baseline configuration as an integral part of information system component installations.	The configuration of the information system is consistent with the Federal Enterprise Architecture and the organization's information system architecture. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).
CM-3	CONFIGURATION CHANGE CONTROL	The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.	Configuration change control involves the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. The organization includes emergency changes in the configuration change control process.
CM-4	MONITORING CONFIGURATION CHANGES	The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.	The organization documents the installation of information system components. After the information system is changed, the organizations checks the security features to ensure the features are still functioning properly. The organization audits activities associated with configuration changes to the information system.
CM-5	ACCESS RESTRICTIONS FOR CHANGE	The organization enforces access restrictions associated with changes to the information system.	None.
CM-6	CONFIGURATION SETTINGS	The organization configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.	NIST Special Publication 800-70 provides guidance on configuration settings (i.e., checklists) for information technology products.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
CM-7	LEAST FUNCTIONALITY	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*].	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). The functions and services provided by information systems should be 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).
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	The contingency planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
CP-2	CONTINGENCY PLAN	The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel. The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).	None.
CP-3	CONTINGENCY TRAINING	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
CP-4	CONTINGENCY PLAN TESTING	The organization tests the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions. The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).	There are several methods for testing contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises).
CP-5	CONTINGENCY PLAN UPDATE	The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
CP-6	ALTERNATE STORAGE SITES	The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
CP-7	ALTERNATE PROCESSING SITES	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*] when the primary processing capabilities are unavailable. The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards. 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. Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.	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.
CP-8	TELECOMMUNICATIONS SERVICES	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*] when the primary telecommunications capabilities are unavailable. 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.	In the event that the primary and/or alternate telecommunications services are provided by a wireline carrier, the organization should ensure that it 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).

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
CP-9	INFORMATION SYSTEM BACKUP	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and stores backup information at an appropriately secured location. The organization tests backup information [*Assignment: organization-defined frequency*] to ensure media reliability and information integrity.	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.
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization employs 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.	Secure information system recovery and reconstitution to the system's original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, and the system is fully tested.
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73 and 800-76; and (ii) other applicable federal laws, 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.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
IA-2	USER IDENTIFICATION AND AUTHENTICATION	The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein. FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication. For other than remote situations, when users identify and authenticate to information systems within a specified security perimeter which is considered to offer sufficient protection, NIST Special Publication 800-63 guidance should be applied as follows: (i) for low-impact information systems, tokens that meet Level 1, 2, 3, or 4 requirements are acceptable; (ii) for moderate-impact information systems, tokens that meet Level 2, 3, or 4 requirements are acceptable; and (iii) for high-impact information systems, tokens that meet Level 3 or 4 requirements are acceptable. In addition to identifying and authenticating users at the information system level, identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	The information system identifies and authenticates specific devices before establishing a connection.	The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.
IA-4	IDENTIFIER MANAGEMENT	The organization manages 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 [*Assignment: organization-defined time period*] of inactivity; and (vi) archiving user identifiers.	Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
IA-5	AUTHENTICATOR MANAGEMENT	The organization manages 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.	Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. FIPS 201 and Special Publications 800-73 and 800-76 specify a personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
IA-6	AUTHENTICATOR FEEDBACK	The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.	The information system may obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	The incident response policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-12 provides guidance on security policies and procedures.
IR-2	INCIDENT RESPONSE TRAINING	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*].	None.
IR-3	INCIDENT RESPONSE TESTING	The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and exercises*] to determine the incident response effectiveness and documents the results.	None.
IR-4	INCIDENT HANDLING	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The organization employs automated mechanisms to support the incident handling process.	The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.
IR-5	INCIDENT MONITORING	The organization tracks and documents information system security incidents on an ongoing basis.	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
IR-6	INCIDENT REPORTING	The organization promptly reports incident information to appropriate authorities. The organization employs automated mechanisms to assist in the reporting of security incidents.	The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.
IR-7	INCIDENT RESPONSE ASSISTANCE	The organization provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability. The organization employs automated mechanisms to increase the availability of incident response-related information and support.	Possible implementations of incident support resources in an organization include a help desk or an assistance group and access to forensics services, when required.
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	The information system maintenance policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance 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.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
MA-2	PERIODIC MAINTENANCE	The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization maintains a maintenance log for the information system 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).	Appropriate organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks the security features to ensure that they are still functioning properly.
MA-3	MAINTENANCE TOOLS	The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
MA-4	REMOTE MAINTENANCE	The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.	The organization describes the use of remote diagnostic tools in the security plan for the information system. The organization maintains maintenance logs for all remote maintenance, diagnostic, and service activities. Appropriate organization officials periodically review maintenance logs. Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections. If password-based authentication is used during remote maintenance, the organization changes the passwords following each remote maintenance service. For high-impact information systems, if remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems before the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
MA-5	MAINTENANCE PERSONNEL	The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.	Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.
MA-6	TIMELY MAINTENANCE	The organization obtains maintenance support and spare parts for [*Assignment: organization-defined list of key information system components*] within [*Assignment: organization-defined time period*] of failure.	None.
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	The media protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection 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.
MP-2	MEDIA ACCESS	The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
MP-3	MEDIA LABELING	The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The organization exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: [*Assignment: organization-defined list of media types and hardware components*].	The organization marks human-readable output appropriately in accordance with applicable policies and procedures. At a minimum, the organization affixes printed output that is not otherwise appropriately marked, with cover sheets and labels digital media with the distribution limitations, handling caveats, and applicable security markings, if any, of the information.
MP-4	MEDIA STORAGE	The organization physically controls and securely stores information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.	The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. The organization protects unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately labeled.
MP-5	MEDIA TRANSPORT	The organization controls information system media (paper and digital) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
MP-6	MEDIA SANITIZATION	The organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.	Sanitization is the process used to remove information from digital media such that information recovery is not possible. Sanitization includes removing all labels, markings, and activity logs. Sanitization techniques, including degaussing and overwriting memory locations, ensure that organizational information is not disclosed to unauthorized individuals when such media is reused or disposed. The National Security Agency maintains a listing of approved products at http://www.nsa.gov/ia/government/mdg.cfm with degaussing capability. The product selected is appropriate for the type of media being degaussed. NIST Special Publication 800-36 provides guidance on appropriate sanitization equipment, techniques and procedures.
MP-7	MEDIA DESTRUCTION AND DISPOSAL	The organization sanitizes or destroys 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.	The organization: (i) sanitizes information system hardware and machine-readable media using approved methods before being released for reuse outside of the organization; or (ii) destroys the hardware/media. Media destruction and disposal should be accomplished in an environmentally approved manner. The National Security Agency provides media destruction guidance at http://www.nsa.gov/ia/government/mdg.cfm. The organization destroys information storage media when no longer needed in accordance with organization-approved methods and organizational policy and procedures. The organization tracks, documents, and verifies media destruction and disposal actions. The organization physically destroys nonmagnetic (optical) media (e.g., compact disks, digital video disks) in a safe and effective manner. NIST Special Publication 800-36 provides guidance on appropriate sanitization equipment, techniques and procedures.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	The physical and environmental protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection 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.
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	The organization develops and keeps 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 issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials [*Assignment: organization-defined frequency, at least annually*].	The organization promptly removes personnel no longer requiring access from access lists.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
PE-3	PHYSICAL ACCESS CONTROL	The organization controls 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 verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.	The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. After an emergency-related event, the organization restricts reentry to facilities to authorized individuals only. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled.
PE-5	ACCESS CONTROL FOR DISPLAY MEDIUM	The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.	None.
PE-6	MONITORING PHYSICAL ACCESS	The organization monitors physical access to information systems to detect and respond to incidents. The organization monitors real-time intrusion alarms and surveillance equipment.	The organization reviews physical access logs periodically, investigates apparent security violations or suspicious physical access activities, and takes remedial actions.
PE-7	VISITOR CONTROL	The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible. The organization escorts visitors and monitors visitor activity, when required.	Government contractors and others with permanent authorization credentials are not considered visitors.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
PE-8	ACCESS LOGS	The organization maintains 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 [*Assignment: organization-defined frequency*] after closeout. The organization employs automated mechanisms to facilitate the maintenance and review of access logs.	None.
PE-9	POWER EQUIPMENT AND POWER CABLING	The organization protects power equipment and power cabling for the information system from damage and destruction.	None.
PE-10	EMERGENCY SHUTOFF	For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology 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.	None.
PE-11	EMERGENCY POWER	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
PE-12	EMERGENCY LIGHTING	The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.	None.
PE-13	FIRE PROTECTION	The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire. Fire suppression and detection devices/systems activate automatically in the event of a fire.	Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.	None.
PE-15	WATER DAMAGE PROTECTION	The organization protects 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.	None.
PE-16	DELIVERY AND REMOVAL	The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.	The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized access. Appropriate organizational officials authorize the delivery or removal of information system-related items belonging to the organization.
PE-17	ALTERNATE WORK SITE	Individuals within the organization employ appropriate information system security controls at alternate work sites.	NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications. The organization provides a means for employees to communicate with information system security staff in case of security problems.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
PL-1	**SECURITY PLANNING POLICY AND PROCEDURES**	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	The security planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security planning policy can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.
PL-2	**SYSTEM SECURITY PLAN**	The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	NIST Special Publication 800-18 provides guidance on security planning.
PL-3	**SYSTEM SECURITY PLAN UPDATE**	The organization reviews the security plan for the information system [*Assignment: organization-defined frequency*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	Significant changes are defined in advance by the organization and identified in the configuration management process.
PL-4	**RULES OF BEHAVIOR**	The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.	Electronic signatures are acceptable for use in acknowledging rules of behavior. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
PL-5	PRIVACY IMPACT ASSESSMENT	The organization conducts a privacy impact assessment on the information system.	OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	The personnel security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security 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.
PS-2	POSITION CATEGORIZATION	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*].	Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.
PS-3	PERSONNEL SCREENING	The organization screens individuals requiring access to organizational information and information systems before authorizing access.	Screening is consistent with: (i) 5 CFR 731.106(a); (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73 and 800-76; and (v) the criteria established for the risk designation of the assigned position.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
PS-4	PERSONNEL TERMINATION	When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.	None.
PS-5	PERSONNEL TRANSFER	The organization reviews 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).	None.
PS-6	ACCESS AGREEMENTS	The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access.	None.
PS-7	THIRD-PARTY PERSONNEL SECURITY	The organization establishes 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) and monitors provider compliance to ensure adequate security.	The organization explicitly includes personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
PS-8	PERSONNEL SANCTIONS	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	The sanctions process is consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	The risk assessment policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.
RA-2	SECURITY CATEGORIZATION	The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.	NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. The organization conducts security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners.
RA-3	RISK ASSESSMENT	The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.	Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
RA-4	RISK ASSESSMENT UPDATE	The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.	The organization develops and documents specific criteria for what is considered significant change to the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.
RA-5	VULNERABILITY SCANNING	Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency*] or when significant new vulnerabilities affecting the system are identified and reported.	The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. 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 provides guidance on handling security patches.
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, 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.	The system and services acquisition policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SA-2	ALLOCATION OF RESOURCES	The organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system.	The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process.
SA-3	LIFE CYCLE SUPPORT	The organization manages the information system using a system development life cycle methodology that includes information security considerations.	NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SA-4	ACQUISITIONS	The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.	*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; (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 800-53 provides guidance on recommended security controls for federal information systems to meet minimum security requirements for information systems categorized in accordance with FIPS 199. 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. *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. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SA-5	INFORMATION SYSTEM DOCUMENTATION	The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel. The organization includes documentation describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.	Administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) optimizing the system's security features. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.
SA-6	SOFTWARE USAGE RESTRICTIONS	The organization complies with software usage restrictions.	Software and associated documentation is used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
SA-7	USER INSTALLED SOFTWARE	The organization enforces explicit rules governing the downloading and installation of software by users.	If provided the necessary privileges, users have the ability to download and install software. The organization identifies what types of software downloads and installations are permitted (e.g., updates and security patches to existing software) and what types of downloads and installations are prohibited (e.g., software that is free only for personal, not government, use). The organization also restricts the use of install-on-demand software.
SA-8	SECURITY DESIGN PRINCIPLES	The organization designs and implements the information system using security engineering principles.	NIST Special Publication 800-27 provides guidance on engineering principles for information system security.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SA-9	**OUTSOURCED INFORMATION SYSTEM SERVICES**	The organization ensures 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. The organization monitors security control compliance.	Third-party providers are subject to the same information system security policies and procedures of the supported organization, and must conform to the same security control and documentation requirements as would apply to the organization's internal systems. Appropriate organizational officials approve outsourcing of information system services to third-party providers (e.g., service bureaus, contractors, and other external organizations). The outsourced information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service level agreements. Service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle.
SA-11	**DEVELOPER SECURITY TESTING**	The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.	Developmental security test results should only be used when no security relevant modifications of the information system have been made subsequent to developer testing and after selective verification of developer test results.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, 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.	The system and communications protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection 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.
SC-2	APPLICATION PARTITIONING	The information system separates user functionality (including user interface services) from information system management functionality.	The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.
SC-4	INFORMATION REMNANTS	The information system prevents unauthorized and unintended information transfer via shared system resources.	Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SC-5	DENIAL OF SERVICE PROTECTION	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*].	A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, network perimeter 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.
SC-6	RESOURCE PRIORITY	The information system limits the use of resources by priority.	Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.
SC-7	BOUNDARY PROTECTION	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.	Any connections to the Internet, or other external networks or information systems, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). The operational failure of the boundary protection mechanisms does not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.
SC-8	TRANSMISSION INTEGRITY	The information system protects the integrity of transmitted information.	The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SC-9	TRANSMISSION CONFIDENTIALITY	The information system protects the confidentiality of transmitted information.	The FIPS 199 security category (for confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.
SC-10	NETWORK DISCONNECT	The information system terminates a network connection at the end of a session or after [*Assignment: organization-defined time period*] of inactivity.	None.
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.	NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.
SC-13	USE OF VALIDATED CRYPTOGRAPHY	When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.	NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.
SC-14	PUBLIC ACCESS PROTECTIONS	For publicly available systems, the information system protects the integrity of the information and applications.	None.
SC-15	COLLABORATIVE COMPUTING	The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).	None.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.	Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. NIST Special Publication 800-63 provides guidance on remote electronic authentication.
SC-18	MOBILE CODE	The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.	Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at: http://iase.disa.mil/mcp/index.html.
SC-19	VOICE OVER INTERNET PROTOCOL	The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.	NIST Special Publication 800-58 provides guidance on security considerations for VOIP technologies employed in information systems.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	The system and information integrity policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity 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.
SI-2	FLAW REMEDIATION	The organization identifies, reports, and corrects information system flaws.	The organization identifies information systems containing proprietary or open source software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). Proprietary software can be found in either commercial/government off-the-shelf information technology component products or in custom-developed applications. The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring (see security controls CA-2, CA-4, or CA-7), or incident response activities (see security control IR-4) should also be addressed expeditiously. NIST Special Publication 800-40 provides guidance on security patch installation.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SI-3	MALICIOUS CODE PROTECTION	The information system implements malicious code protection that includes a capability for automatic updates. The organization centrally manages virus protection mechanisms.	The organization employs virus protection mechanisms at critical information system entry and exit 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 virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates virus protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. Consideration is given to using virus protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).
SI-4	INTRUSION DETECTION TOOLS AND TECHNIQUES	The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	Intrusion detection and information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, virus protection software, log monitoring software, network forensic analysis tools).
SI-5	SECURITY ALERTS AND ADVISORIES	The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	The organization documents the types of actions to be taken in response to security alerts/advisories.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SI-6	SECURITY FUNCTIONALITY VERIFICATION	The information system verifies the correct operation of security functions [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: organization-defined time-period*]] *and* [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.	None.
SI-8	SPAM AND SPYWARE PROTECTION	The information system implements spam and spyware protection.	The organization employs spam and spyware 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 and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means. Consideration is given to using spam and spyware protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).
SI-9	INFORMATION INPUT RESTRICTIONS	The organization restricts the information input to the information system to authorized personnel only.	Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

MINIMUM SECURITY CONTROLS
MODERATE BASELINE

CONTROL #	CONTROL NAME	CONTROL	SUPPLEMENTAL GUIDANCE
SI-10	INFORMATION INPUT ACCURACY, COMPLETENESS, AND VALIDITY	The information system checks information inputs for accuracy, completeness, and validity.	Checks for accuracy, completeness, and validity of information should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters should be prescreened to ensure the content is not unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, and validity of information inputs should be guided by organizational policy and operational requirements.
SI-11	ERROR HANDLING	The information system identifies and handles error conditions in an expeditious manner.	The structure and content of error messages should be carefully considered by the organization. User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions should be guided by organizational policy and operational requirements.
SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.	None.