Sample CDC Certification and Accreditation Checklist

For an Application That Is Considered a Moderate Threat

Centers for Disease Control and Prevention

National Center for Chronic Disease Prevention and Health Promotion

Division of Cancer Prevention and Control

National Program of Cancer Registries

November 23, 2009

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Access Control Policy Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	
Account Management	Registry	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts at least annually. Control Enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary and emergency accounts after ...organization-defined time period for each type of account. (3) The information system automatically disables inactive accounts after...organization-defined time period. (4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.	
Response to Audit Processing Failures	Registry	The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	
Information Flow Enforcement	Registry	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	
Separation of Duties	Registry	The information system enforces separation of duties through assigned access authorizations.	
Time Stamps	Registry / Software	The information system provides time stamps for use in audit record generation. Control Enhancements: (1) The organization synchronizes internal information system clocks [organization-defined frequency].	
User Identification and Authentication	Software	The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Related security controls: AC-14, AC-17. Control Enhancements: (1) The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 [Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4] compliant.	
Device Identification and Authentication	Software	The information system identifies and authenticates specific devices before establishing a connection.	
System Security Plan	Software	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.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Session Termination	Registry	The information system automatically terminates a remote session after [organization-defined time period] of inactivity.	
Supervision and Review—Access Control	Registry	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. The organization employs automated mechanisms to facilitate the review of user activities.	
Permitted Actions without Identification or Authentication	Registry	The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication. (1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives. Related security control: IA-2.	
Remote Access	Registry	The organization authorizes, monitors, and controls all methods of remote access to the information system. Related security control: IA-2. Control Enhancements: (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. (3) The organization controls all remote accesses through a limited number of managed access control points. (4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	
Wireless Access Restrictions	Registry	The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system. Control Enhancements: (1) The organization uses authentication and encryption to protect wireless access to the information system.	
Access Control for Portable and Mobile Devices	Registry	The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.	
Use of External Information Systems	Registry	The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system. Control Enhancements: (1) The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Security Awareness and Training Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	
Security Awareness	Registry	The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined frequency, at least annually] thereafter.	
Security Training	Registry	The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [organization-defined frequency] thereafter.	
Security Training Records	Registry	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.	
Audit and Accountability Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	
System Security Plan Update	Software	The organization reviews the security plan for the information system [organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	
Application Partitioning	Software	The information system separates user functionality (including user interface services) from information system management functionality.	
Audit Storage Capacity	Registry	The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. Related security controls: AU-2, AU-5, AU-6, AU-7, SI-4	
Information Remnance	Software	The information system prevents unauthorized and unintended information transfer via shared system resources.	
Audit Monitoring, Analysis, and Reporting	Registry	The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. Control Enhancements: (2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [organization-defined list of inappropriate or unusual activities that are to result in alerts]	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Audit Reduction and Report Generation	Registry	The information system provides an audit reduction and report generation capability. Control Enhancements: (1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.	
Information Accuracy, Completeness, Validity, and Authenticity	Software	The information system checks information for accuracy, completeness, validity, and authenticity	
Protection of Audit Information	Registry	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	
Audit Record Retention	Registry	The organization retains audit records 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.	
Certification, Accreditation, and Security Assessment Policies and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.	
Security Assessments	Registry	The organization conducts an assessment of the security controls in the information system [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.	
Information System Connections	Registry	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.	
Security Certification	Registry	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. Related security controls: CA-2, CA-6, SA-11. Control Enhancements: (1) The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.	
Plan of Action and Milestones	Registry	The organization develops and updates [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization’s planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Security Accreditation	Registry	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [Assignment: organization-defined frequency, at least every three years] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.	
Continuous Monitoring	Registry	The organization monitors the security controls in the information system on an ongoing basis.	
Configuration Management Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	
Baseline Configuration	Registry	The organization develops, documents, and maintains a current baseline configuration of the information system. Related security controls: CM-6, CM-8. Control Enhancements: (1) The organization updates the baseline configuration of the information system as an integral part of information system component installations.	
Configuration Change Control	Registry	The organization authorizes, documents, and controls changes to the information system.	
Monitoring Configuration Changes	Registry	The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.	
Access Restrictions for Change	Registry	The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.	
Configuration Settings	Registry	The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.	
Least Functionality	Registry	The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.	
Information System Component Inventory	Registry	The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. Related security controls: CM-2, CM-6. Control Enhancements: (1) The organization updates the inventory of information system components as an integral part of component installations.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Contingency Planning Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	
Contingency Plan	Registry	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. Control Enhancements: (1) The organization coordinates contingency plan development with organizational elements responsible for related plans. Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.	
Contingency Training	Registry	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].	
Contingency Plan Testing and Exercises	Registry	The organization: (i) tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan’s effectiveness and the organization’s readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions. Control Enhancements: (1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	
Contingency Plan Update	Registry	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.	
Alternate Storage Site	Registry	The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. Control Enhancements: (1) The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards. (3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Alternate Processing Site	Registry	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. Control Enhancements: (1) The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards. (2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. (3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	
Telecommunications Services	Registry	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. Control Enhancements: (1) The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. (2) The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.	
Information System Backup	Registry	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [organization-defined frequency] and protects backup information at the storage location. Related security controls: MP-4, MP-5. Control Enhancements: (1) The organization tests backup information [organization-defined frequency] to verify media reliability and information integrity. (4) The organization protects system backup information from unauthorized modification.	
Information System Recovery and Reconstitution	Registry	The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.	
Error Handling	Software	The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.	
Information System Documentation	Software	The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Control Enhancements: (1) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls	
Auditable Events	Registry / Software	The information system generates audit records for the following events: [organization-defined auditable events]. Control Enhancements: (3) The organization periodically reviews and updates the list of organization-defined auditable events.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Identifier Management	Registry	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) issuing the user identifier to the intended party; (v) disabling the user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.	
Authenticator Management	Registry	The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	
Authenticator Feedback	Registry	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	
Cryptographic Module Authentication	Registry	The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	
Incident Response Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	
Incident Response Training	Registry	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].	
Incident Response Testing and Exercises	Registry	The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.	
Incident Handling	Registry	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Related security controls: AU-6, PE-6. Control Enhancements: (1) The organization employs automated mechanisms to support the incident handling process.	
Incident Monitoring	Registry	The organization tracks and documents information system security incidents on an ongoing basis.	
Incident Reporting	Registry	The organization promptly reports incident information to appropriate authorities.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Incident Response Assistance	Registry	The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability. Control Enhancements: (1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	
System Maintenance Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	
Controlled Maintenance	Registry	The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. Control Enhancements: The organization maintains maintenance records for the information system that include: (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).	
Maintenance Tools	Registry	The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.	
Remote Maintenance	Registry	The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed. Control Enhancements: (1) The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions. (2) The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.	
Maintenance Personnel	Registry	The organization allows only authorized personnel to perform maintenance on the information system.	
Timely Maintenance	Registry	The organization obtains maintenance support and spare parts for [organization-defined list of key information system components] within [organization-defined time period] of failure.	
Media Protection Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	
Media Access	Registry	The organization restricts access to information system media to authorized individuals. Control Enhancements: The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Media Storage	Registry	The organization physically controls and securely stores information system media within controlled areas.	
Media Transport	Registry	The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. Control Enhancements: (1) The organization protects digital and non-digital media during transport outside of controlled areas using [organization-defined security measures, e.g., locked container, cryptography]. (2) The organization documents, where appropriate, activities associated with the transport of information system media using [organization-defined system of records]. Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.	
Media Sanitization and Disposal	Registry	The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.	
Physical and Environmental Protection Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	
Physical Access Authorizations	Registry	The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].	
Physical Access Control	Registry	The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.	
Access Control for Display Medium	Registry	The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.	
Monitoring Physical Access	Registry	The organization monitors physical access to the information system to detect and respond to physical security incidents. Control Enhancements: (1) The organization monitors real-time physical intrusion alarms and surveillance equipment.	
Visitor Control	Registry	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. Control Enhancements: (1) The organization escorts visitors and monitors visitor activity, when required.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Access Records	Registry	The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency].	
Power Equipment and Power Cabling	Registry	The organization protects power equipment and power cabling for the information system from damage and destruction.	
Emergency Shutoff	Registry	The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.	
Emergency Power	Registry	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.	
Emergency Lighting	Registry	The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.	
Fire Protection	Registry	The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire. Control Enhancements: (1) The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire. (2) The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders. (3) The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.	
Temperature and Humidity Controls	Registry	The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.	
Water Damage Protection	Registry	The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	
Delivery and Removal	Registry	The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items. Supplemental Guidance: The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.	
Alternate Work Site	Registry	The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.	
Location of Information System Components	Registry	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Security Planning Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	
Content of Audit Records	Software	The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Control Enhancements: (1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	
System Use Notification	Software	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.	
Rules of Behavior	Registry	The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.	
Session Lock	Software	The information system prevents further access to the system by initiating a session lock after [organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	
Security-Related Activity Planning	Registry	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	
Personnel Security Policy and Procedures	Registry	The organization reviews the security plan for the information system [organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	
Position Categorization	Registry	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].	
Personnel Screening	Registry	The organization screens individuals requiring access to organizational information and information systems before authorizing access.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Personnel Termination	Registry	The organization screens individuals requiring access to organizational information and information systems before authorizing access.	
Personnel Transfer	Registry	The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.	
Access Agreements	Registry	The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [Assignment: organization-defined frequency].	
Third-Party Personnel Security	Registry	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.	
Personnel Sanctions	Registry	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	
Risk Assessment Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	
Security Categorization	Registry	The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.	
Risk Assessment	Registry	The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).	
Risk Assessment Update	Registry	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.	
Vulnerability Scanning	Registry	The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
System and Services Acquisition Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	
Allocation of Resources	Registry	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.	
Life Cycle Support	Registry	The organization manages the information system using a system development life cycle methodology that includes information security considerations.	
Identification and Authentication Policy and Procedures	Software	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	
Access Enforcement	Software	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. See Supplemental Guidance. Control Enhancements: (1) The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).	
Software Usage Restrictions	Registry	The organization complies with software usage restrictions.	
User Installed Software	Registry	The organization enforces explicit rules governing the installation of software by users.	
Information Input Restrictions	Software	The organization restricts the capability to input information to the info system to authorized personnel.	
External Information System Services	Registry	The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.	
Developer Security Testing	Registry	The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results. Related security controls: CA-2, CA-4.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
System and Communications Protection Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	
Security Engineering Principles	Software	The organization designs and implements the information system using security engineering principles.	
Privacy Impact Assessment	Software	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	
Denial of Service Protection	Registry	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].	
Boundary Protection	Registry	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. Related security controls: MP-4, RA-2. Control Enhancements: (1) The organization physically allocates publicly accessible information system components to separate sub networks with separate, physical network interfaces. (2) The organization prevents public access into the organization's internal networks except as appropriately mediated. (3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. (4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. (5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). (6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	
Transmission Integrity	Registry	The information system protects the integrity of transmitted information.	
Transmission Confidentiality	Registry	The information system protects the confidentiality of transmitted information.	
Network Disconnect	Registry	The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.	
Cryptographic Key Establishment and Management	Registry	When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Use of Cryptography	Registry	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
Public Access Protections	Registry	The information system protects the integrity and availability of publicly available information and applications.	
Collaborative Computing	Registry	The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.	
Public Key Infrastructure Certificates	Registry	The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	
Mobile Code	Registry	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) authorizes, monitors, and controls the use of mobile code within the information system.	
Voice Over Internet Protocol	Registry	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) authorizes, monitors, and controls the use of VoIP within the information system.	
Secure Name /Address Resolution Service (Authoritative Source)	Registry	The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.	
Architecture and Provisioning for Name/Address Resolution Service	Registry	The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.	
Session Authenticity	Registry	The information system provides mechanisms to protect the authenticity of communications sessions.	
System and Information Integrity Policy and Procedures	Registry	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	
Flaw Remediation	Registry	The organization identifies, reports, and corrects information system flaws. Control Enhancements: The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.	

Moderate Control Name	Control	NIST Control See Supplemental Guidance for More Detail of Each Control	Method(s) Used to Address NIST Control
Malicious Code Protection	Registry	The information system implements malicious code protection. Control Enhancements: (1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms.	
Information System Monitoring Tools and Techniques	Registry	The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. Control Enhancements: (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	
Security Alerts and Advisories	Registry	The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	
Spam Protection	Registry	The information system implements spam protection.	
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 and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. Control Enhancements: (1) The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.	
Unsuccessful Login Attempts	Registry / Software	The information system enforces a limit of [organization-defined number] consecutive invalid access attempts by a user during a [organization-defined] time period. The information system automatically [Selection: locks the account/node for a [defined time period], delays next login prompt according to [defined delay algorithm.] when the maximum number of unsuccessful attempts is exceeded.	
Least Privilege	Software	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.	
Information Output Handling and Retention	Registry	The organization handles and retains outputs from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	