

MODERATE-LEVEL SYSTEM SECURITY CONTROL ASSESSMENT

Below is a list of security controls for a moderate controlled system and their objectives. If the control has been specifically implemented for the EFM system place an "X" in the column titled "In Place". Control numbers are listed in sequential order and control numbers that are not applicable to a moderate-level system have been deleted.

Control Number	Control	In Place
Access Controls (AC)		
AC-1	Access Control Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	
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 annually.	
AC-3	Access Enforcement: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	
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.	
AC-5	Separation of Duties: The information system enforces separation of duties through assigned access authorizations.	
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.	
AC-7	Unsuccessful Logon Attempts: The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account/node for 30 minutes for low systems or until an appropriate security administrator manually intervenes to unlock accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.	

Control Number	Control	In Place
AC-8	System Use Notification: The information system displays an approved, system use notification message before granting system access informing potential users: (1) that the user is accessing a U.S. Government information system; (2) that system usage may be monitored, recorded, and subject to audit; (3) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (4) 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.	
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.	
AC-12	Session Termination: The information system automatically terminates a session after ten minutes of inactivity.	
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.	
AC-14	Permitted Actions w/o Identification or Authentication: The organization identifies specific user actions that can be performed on the information system without identification or authentication.	
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.	
AC-18	Wireless Access Restrictions: The organization: (1) establishes usage restrictions and implementation guidance for wireless technologies; and (2) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.	
AC-19	Access Control for Portable and Mobile Systems: The organization: (1) establishes usage restrictions and implementation guidance for portable and mobile devices; and (2) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.	
AC-20	Use of External 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.	

Control Number	Control	In Place
Awareness and Training (AT)		
AT-1	Security Awareness and Training Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	
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 at least annually thereafter.	
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 each year thereafter.	
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.	
Audit and Accountability (AU)		
AU-1	Audit and Accountability Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	
AU-2	Auditable Events: The information system generates audit records for events identified in the WFS IT Security Handbook.	
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.	
AU-4	Audit Storage Capacity: The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.	

Control Number	Control	In Place
AU-5	<p>Response to Audit Processing Failures: 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:</p> <ul style="list-style-type: none"> • Shutdown the system • Overwrite the oldest audit records • Stop generating audit records 	
AU-6	<p>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.</p>	
AU-7	<p>Audit Reduction and Report Generation: The information system provides an audit reduction and report generation capability.</p>	
AU-8	<p>Time Stamps: The information system provides time stamps for use in audit record generation.</p>	
AU-9	<p>Protection of Audit Information: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.</p>	
AU-11	<p>Audit Retention: The organization retains audit logs in accordance with WFS records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.</p>	
Certification, and Accreditation, and Security Assessments(CA)		
CA-1	<p>Certification, Accreditation, and Security Assessment Policies and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.</p>	
CA-2	<p>Security Assessments: The organization conducts an assessment of the security controls in the information system 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.</p>	
CA-3	<p>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.</p>	

Control Number	Control	In Place
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.	
CA-5	Plan of Action and Milestones: The organization develops and updates quarterly, 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.	
CA-6	Security Accreditation: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.	
CA-7	Continuous Monitoring: The organization monitors the security controls in the information system on an ongoing basis.	
Configuration Management (CM)		
CM-1	Configuration Management Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	
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.	
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.	
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.	
CM-5	Access Restrictions for Change: The organization enforces access restrictions associated with changes to the information system.	
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.	

Control Number	Control	In Place
CM-7	Least Functionality: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of any protocol or service that is not explicitly permitted.	
CM-8	Information System Component Inventory: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.	
Contingency Planning (CP)		
CP-1	Contingency Planning Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	
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.	
CP-3	Contingency Training: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.	
CP-4	Contingency Plan Testing and Exercises: The organization tests the contingency plan for the information system at least annually using to determine the plan's effectiveness and the organization's readiness to execute the plan. System rated as high shall be tested at the alternate processing site. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.	
CP-5	Contingency Plan Update: The organization reviews the contingency plan for the information system once per year and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	
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.	
CP-7	Alternate Processing Site: 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 24 hours when the primary processing capabilities are unavailable.	

Control Number	Control	In Place
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 24 hours when the primary telecommunications capabilities are unavailable.	
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 according to backup schedules documented in the system contingency plan and stores backup information at an appropriately secured location.	
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.	
Identification and Authentication (IA)		
IA-1	Identification and Authentication Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	
IA-2	User Identification and Authentication: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	
IA-3	Device Identification and Authentication: The information system identifies and authenticates specific devices before establishing a connection.	
IA-4	Identifier Management: The organization manages user identifiers by: (1) uniquely identifying each user; (2) verifying the identity of each user; (3) receiving authorization to issue a user identifier from an appropriate organization official; (4) ensuring that the user identifier is issued to the intended party; (5) disabling user identifier after 30 days of inactivity; and (6) archiving user identifiers.	
IA-5	Authenticator Management: The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (1) defining initial authenticator content; (2) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (3) changing default authenticators upon information system installation.	
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.	

Control Number	Control	In Place
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.	
Incident Response (IR)		
IR-1	Incident Response Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	
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 at least annually.	
IR-3	Incident Response Testing and Exercises: The organization tests the incident response capability for the information system at least annually using automated mechanisms for high systems to determine the incident response effectiveness and documents the results.	
IR-4	Incident Handling: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	
IR-5	Incident Monitoring: The organization tracks and documents information system security incidents on an ongoing basis.	
IR-6	Incident Reporting: The organization promptly reports incident information to appropriate authorities.	
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.	
Maintenance (MA)		
MA-1	System Maintenance Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	

Control Number	Control	In Place
MA-2	Controlled 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.	
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.	
MA-4	Remote Maintenance: The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.	
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.	
MA-6	Timely Maintenance: The organization obtains maintenance support and spare parts within 48 hours of failure.	
Media Protection (MP)		
MP-1	Media Protection Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	
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.	
MP-4	Media Storage: The organization physically controls and securely stores information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.	
MP-5	Media Transport: The organization controls information system media (paper and electronic) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.	
MP-6	Media Sanitization and Disposal: 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.	

Control Number	Control	In Place
Physical and Environmental Protection (PE)		
PE-1	Physical and Environmental Protection Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	
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 once a year.	
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.	
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.	
PE-6	Monitoring Physical Access: The organization monitors physical access to information systems to detect and respond to incidents.	
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.	
PE-8	Access Records: The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (1) name and organization of the person visiting; (2) signature of the visitor; (3) form of identification; (4) date of access; (5) time of entry and departure; (6) purpose of visit; and (7) name and organization of person visited. Visitor logs are reviewed at closeout, maintained on file, and available for further review for one year.	
PE-9	Power Equipment and Power Cabling: The organization protects power equipment and power cabling for the information system from damage and destruction.	

Control Number	Control	In Place
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.	
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.	
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.	
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.	
PE-14	Temperature and Humidity Controls: The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.	
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.	
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.	
PE-18	Location of Information System Components: 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.	
Planning (PL)		
PL-1	Security Planning Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	

Control Number	Control	In Place
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.	
PL-3	System Security Plan Update: The organization reviews the security plan for the information system annually and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	
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.	
PL-5	Privacy Impact Assessment: The organization conducts a privacy impact assessment on the information system.	
PL-6	Security-Related Activity Planning: 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.	
Personal Security (PS)		
PS-1	Personnel Security Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	
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 periodically in accordance with OPM guidance.	
PS-3	Personnel Screening: The organization screens individuals requiring access to organizational information and information systems before authorizing access.	

Control Number	Control	In Place
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.	
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).	
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.	
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.	
PS-8	Personnel Sanctions: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	
Risk Assessment		
RA-1	Risk Assessment Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	
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.	
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.	

Control Number	Control	In Place
RA-4	Risk Assessment Update: The organization updates the risk assessment every three years 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.	
RA-5	Vulnerability Scanning: Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system every six months or when significant new vulnerabilities affecting the system are identified and reported.	
System and Services Acquisition (SA)		
SA-1	System and Services Acquisition Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	
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.	
SA-3	Life Cycle Support: The organization manages the information system using a system development life cycle methodology that includes information security considerations.	
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.	
SA-5	Information System Documentation: The organization ensures that adequate documentation for the information system and its constituent components are available, protected when required, and distributed to authorized personnel.	
SA-6	Software Usage Restrictions: The organization complies with software usage restrictions.	
SA-7	User Installed Software: The organization enforces explicit rules governing the downloading and installation of software by users.	
SA-8	Security Engineering Principles: The organization designs and implements the information system using security engineering principles.	

Control Number	Control	In Place
SA-9	External 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.	
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.	
System and Communication Protection (SC)		
SC-1	System & Communications Protection Policy & Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	
SC-2	Application Partitioning: The information system separates user functionality (including user interface services) from information system management functionality.	
SC-4	Information Remnance: The information system prevents unauthorized and unintended information transfer via shared system resources.	
SC-5	Denial of Service Protection: The information system protects against or limits the effects of denial of service attacks on devices within the organization’s internal network.	
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.	
SC-8	Transmission Integrity: The information system protects the integrity of transmitted information.	
SC-9	Transmission Confidentiality: The information system protects the confidentiality of transmitted information.	
SC-10	Network Disconnect: The information system terminates a network connection at the end of a session or after ten minutes of inactivity.	

Control Number	Control	In Place
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.	
SC-13	Use of 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.	
SC-14	Public Access Protections: For publicly available systems, the information system protects the integrity of the information and applications.	
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).	
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.	
SC-18	Mobile Code: The organization: (1) 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 (2) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.	
SC-19	Voice Over Internet Protocol: The organization: (1) 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 (2) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.	
SC-20	Secure Name/Address Resolution Service (Authoritative Source): 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.	
SC-22	Architecture and Provisioning For Name/Address Resolution Service: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.	
SC-23	Session Authenticity: The information system provides mechanisms to protect the authenticity of communications sessions.	

Control Number	Control	In Place
System and Information Integrity (SI)		
SI-1	System and Information Integrity Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	
SI-2	Flaw Remediation: The organization identifies, reports, and corrects information system flaws.	
SI-3	Malicious Code Protection: The information system implements malicious code protection that includes a capability for automatic updates.	
SI-4	Information System Monitoring 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.	
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.	
SI-8	Spam and Spyware Protection: The information system implements spam and spyware protection.	
SI-9	Information Input Restrictions: The organization restricts the information input to the information system to authorized personnel only.	
SI-10	Information Input Accuracy, Completeness, and Validity: The information system checks information inputs for accuracy, completeness, and validity.	
SI-11	Error Handling: The information system identifies and handles error conditions in an expeditious manner.	
SI-12	Output Handling and Retention: The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.	